Consejo de la Unión Europea

Bruselas, 5 de septiembre de 2019
(OR. en)

9364/19

DAPIX 184
ENFOPOL 252
CT 53
ENFOCUSTOM 105
CRIMORG 81
SCHENGEN 23
VISA 116
SIRIS 97
COPEN 219
ASIM 62
FRONT 190
COMIX 273
JAI 529

NOTA

De:	Secretaría General del Consejo
A:	Grupo «Intercambio de Información y Protección de Datos» (DAPIX)
N.º doc. prec.:	6727/18
Asunto:	Manual para el intercambio de información en el ámbito policial

1. Introducción

El Manual para el intercambio de información en el ámbito policial tiene por objeto completar el Manual sobre operaciones transfronterizas (10505/4/09 REV 4). Tanto el contenido y la estructura del manual como las fichas nacionales han sido aprobadas por el Grupo DAPIX en el marco de la Estrategia de gestión de la información para la seguridad interior de la UE (IMS), con miras a apoyar, racionalizar y facilitar el intercambio de información transfronterizo.

Para reforzar su valor práctico, el manual estará disponible en todas las lenguas oficiales de la Unión. Asimismo, se actualizará dos veces al año, conforme sea necesario a la luz de la nueva legislación o la experiencia práctica.

La actual versión recoge, en particular, las novedades relativas al Reglamento Europol y a los datos de contacto. Los Estados miembros actualizan periódicamente los datos de contacto y los consignan en las fichas nacionales, que a partir de ahora aparecerán como adenda (ADD 1) del manual. Dicha adenda incluye información sensible y no puede ser divulgada sin consultar a la SGC, en consonancia con lo dispuesto en el Reglamento (CE) n.º 1049/2001[1]. Un elemento nuevo son las recomendaciones prácticas (ADD 2), que ofrecen una comparación de los requisitos para el intercambio de información por medio de diferentes canales.

2. Propósito del manual

El manual está concebido ante todo como una herramienta para los agentes de policía que trabajan en el ámbito de los enlaces internacionales y, en primer lugar, para los denominados **operadores de los «PUC».** En consecuencia, debe ser lo más fácil de usar y lo más completo posible.

El manual tiene por objeto informar y facilitar la **cooperación práctica cotidiana** entre las autoridades de los distintos Estados miembros que intervienen en el intercambio de información policial tanto en el ámbito nacional como en el internacional, para ser utilizado con fines de formación y garantizar que se tomen las decisiones con mejor información cuando se trate de solicitar e intercambiar información de un Estado a otro.

El manual contiene **una visión general de todos los sistemas, bases jurídicas e instrumentos de intercambio de información de la UE,** a disposición de las autoridades policiales de los Estados miembros. De este modo, el usuario queda plenamente informado de las posibilidades de que dispone a la hora de decidir cómo solicitar o facilitar información de un Estado a otro.

Completan el manual unas **fichas nacionales** en las que figuran los datos de contacto relevantes y la información disponible para el intercambio transfronterizo. Al actualizar periódicamente estas fichas, los Estados miembros habrán cumplido las diversas obligaciones de notificación que les imponen los diferentes instrumentos. Estas fichas nacionales deberán facilitar la gestión y la búsqueda de la información necesaria.

[1] Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión. El Reglamento establece los principios generales y los límites de acceso.

El manual incluye dichas fichas nacionales así como la información práctica esencial relativa a la Decisión Marco 2006/960/JAI del Consejo («Decisión Marco sueca») y sustituye a las antiguas directrices de dicha Decisión Marco (9512/10 CRIMORG 90 ENFOPOL 125 ENFOCUSTOM 36 COMIX 346).

3. Contenido del manual

El manual consta de tres partes que están redactadas de modo que puedan consultarse por separado, según la intención del lector.

La primera parte del manual consta de unas **listas de comprobación** que presentan una visión global pragmática de las posibilidades de intercambio de información y los aspectos prácticos relativos al mismo. Estas listas de comprobación contribuyen a orientar al usuario hacia el punto de contacto adecuado para el intercambio de información basándose en unas lisas de sistemas y métodos disponibles dentro de los siguientes contextos operativos principales:

– la prevención y persecución de delitos (y la inmigración irregular);

– la lucha contra el terrorismo;

– el mantenimiento del orden público y la seguridad.

En segundo lugar, en una descripción **general** se presenta tanto los órganos nacionales que intervienen en el intercambio de información como los instrumentos de dicho intercambio. El manual hace referencia al papel central que desempeñan la Decisión Marco 2006/960/JAI del Consejo («Decisión Marco sueca») y la Decisión 2008/615/JAI del Consejo («Decisión Prüm») en el ámbito general del intercambio de información de la UE. No obstante, el manual no se reduce a estos instrumentos.

En la adenda, el manual se completa con

a) una recopilación de **fichas nacionales** de cada Estado miembro, que contienen los **datos prácticos de los puntos de contacto** importantes para el intercambio de información transfronterizo, y

b) los requisitos para el intercambio de información teniendo en cuenta los distintos canales que se utilizan (Interpol, Europol, Sirene, funcionarios de enlace, CCPA) y recomendaciones más prácticas organizadas de manera sencilla para el usuario.

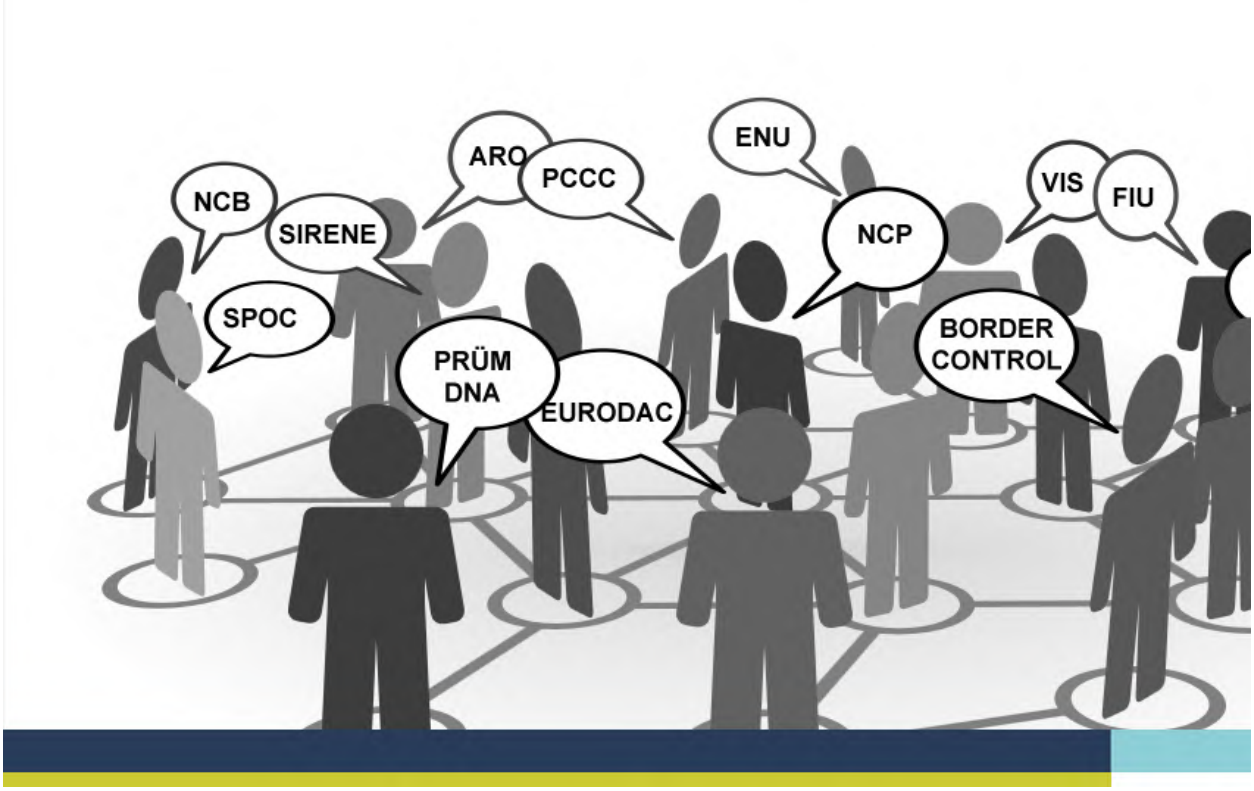
4. Actuación futura

La redacción del manual propuesto se incluyó como punto de acción en la tercera lista de acciones de la Estrategia de gestión de la información, y la primera versión de manual fue elaborada durante las Presidencias irlandesa, chipriota, griega, italiana y letona.

Con el fin de facilitar en mayor medida el uso del Manual para el intercambio de información en el ámbito policial, la Presidencia presenta esta versión actualizada a las Delegaciones y las invita a que la distribuyan de la forma más adecuada a sus necesidades.

Consejo de la Unión Europea
Secretaría General
Dirección General de Justicia y Asuntos de Interior
Dirección de Asuntos de Interior

Manual para el intercambio de información en el ámbito policial



Índice

INTRODUCCIÓN

Propósito de este manual

La cooperación transfronteriza dentro de la Unión Europea reposa muy firmemente en el intercambio de información. El presente manual tiene por objeto facilitar la cooperación cotidiana a este respecto. Está dirigido principalmente al PUC nacional, el punto único de contacto responsable de la gestión del flujo de información entre las distintas unidades y puntos de contacto designados, tanto en el ámbito nacional como en el internacional.

El cuadro de la cooperación policial[2] en Europa se caracteriza por el incremento y la aceleración del intercambio de información. Por una parte, se apoya en unas tecnologías de la información y la comunicación en constante desarrollo. Por otra, existe una plétora de bases de datos disponibles, tanto nacionales como internacionales.

El presente manual se propone atender a la necesidad de hallar el contacto o la base de datos apropiados en un contexto operativo particular. Expone brevemente la legislación correspondiente sin por ello perder de vista su objetivo principal: facilitar el intercambio transfronterizo de información.

Estructura del manual

El manual está dividido en:

La ***PARTE I - «Contexto operativo»*** - consta de una serie de cuadros o «listas de comprobación» que hacen corresponder la información incluida en la *PARTE II* y en la *PARTE III*, bien con la base jurídica correspondiente, bien con la información sobre los puntos de contacto. Estas listas de comprobación están divididas en tres áreas temáticas:

- **prevención y lucha contra la delincuencia (y la inmigración irregular) - lista de comprobación A;**
- **lucha contra los delitos de terrorismo - Lista de comprobación B;**
- **mantenimiento del orden público- Lista de comprobación C.**

El objetivo de estas listas de comprobación es guiar al lector desde el punto escogido como canal o método de comunicación en un contexto operativo particular hasta la fuente de la información de contacto o cualquier acto legislativo, norma o reglamento y manual de mejores prácticas.

[2] A los efectos del presente manual, se entenderá por «policial» la prevención, detección o investigación de delitos de terrorismo, tal como se definen en la Directiva (UE) 2017/541, o de delitos graves, tal como se definen en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI relativa a la orden de detención europea.

La ***PARTE II - «Información general»*** - describe la situación de la acción policial en relación con los diversos métodos y canales de comunicación a disposición de las fuerzas de policía de la UE. Esta segunda parte está, a su vez, desglosada en tres áreas, que tratan de:

- ***los canales de comunicación (es decir los órganos que intervienen en la información policial);***
- ***los sistemas y bases de datos de información utilizados en el intercambio transfronterizo de datos;***
- ***la legislación - el contexto legislativo y las normas y directrices relativas a los principales métodos y sistemas de comunicación.***

La ***Parte III - «Fichas nacionales»***, que se presenta como adenda 1 de este documento, contiene unas fichas nacionales con información detallada sobre los puntos de contacto relevante para todos los aspectos del intercambio de información transfronterizo citados a lo largo del documento. Es responsabilidad de los Estados miembros comunicar rápidamente cualquier cambio a la Secretaría General del Consejo. Al actualizar periódicamente las fichas nacionales en la adenda del manual, los Estados miembros habrán cumplido las diversas obligaciones de notificación que les imponen los diferentes instrumentos. Ello hará más fácil en el futuro gestionar y encontrar esta información.

Parte IV — Recomendaciones prácticas para el intercambio de información en el ámbito policial

La adenda 2 de la presente nota –recomendaciones prácticas– facilita de manera sencilla el cotejo de los requisitos para el intercambio de información por diferentes canales (Interpol, Europol, Sirene, funcionarios de enlace y CCPA). Ofrece además información y recomendaciones prácticas sobre los instrumentos de cooperación policial, que podrían ser de utilidad no solo para los funcionarios de los PUC, sino también para otros cuerpos y fuerzas de seguridad nacionales.

PARTE I - Contexto operativo

LISTA DE COMPROBACIÓN A: INTERCAMBIO DE INFORMACIÓN CON FINES DE PREVENCIÓN Y PERSECUCIÓN DE DELITOS

Sistema de información	**Puntos de acceso nacionales**	**Base jurídica**	**Manual**
Sistema de Información de Schengen - SIS II	Oficinas Sirene («**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry», solicitud de información complementaria a la entrada nacional)	El acervo de Schengen según se contempla en el artículo 1.2 de la Decisión 1999/435/CE del Consejo, de 20 de mayo de 1999, DO L 239 de 22.9.2000, p. 1. Decisión 2007/533/JAI del Consejo, DO L 205 de 7.8.2007, p. 63. Reglamento (CE) n.º 1986/2006, DO L 381 de 28.12.2006, p. 1. Reglamento (CE) n.º 1987/2006, DO L 381 de 28.12.2006, p. 4.	Versión revisada del catálogo actualizado de recomendaciones y prácticas más idóneas para la correcta aplicación del acervo de Schengen, 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484. Decisión de Ejecución (UE) 2017/1528 por la que se sustituye el anexo de la Decisión de Ejecución 2013/115/UE relativa al Manual Sirene y otras medidas de ejecución para el Sistema de Información de Schengen de segunda generación (SIS II), DO L 231 de 7.9.2017, p. 6.

Europol/ Sistema de Información de Europol - Sistema de índice del SIE Ficheros de trabajo de análisis	UNE	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, aplicable desde el 1 de mayo de 2017).	
Interpol I (24 horas al día, 7 días a la semana)	OCN (Oficina Central Nacional)	Reglamento de Interpol sobre el Tratamiento de Datos [III/IRPD/GA/2011(2014)]. Reglamento sobre el Control de la Información y el Acceso a los Ficheros de Interpol [II.E/RCIA/GA/2004(2009)].	
Búsqueda automática ADN/Prüm de las bases de datos nacionales designadas	Punto de contacto nacional 1er paso: búsqueda automática	Decisión 2008/615/JAI del Consejo, DO L 210 de 6.8.2008, p. 1, artículos 3 y 4.	
	2.º paso: transmisión de otros datos de carácter personal y de otras informaciones	Legislación nacional Decisión 2006/960/JAI del Consejo («Decisión Marco sueca»). DO L 386 de 29.12.2006, p. 89. Corrigenda DO L 75 de 15.3.2007, p. 26.	

Búsqueda automática de impresiones dactilares/Prüm de los AFIS nacionales	Punto de contacto nacional 1er paso: búsqueda automática	Decisión 2008/615/JAI del Consejo, artículo 9, DO L 210 de 6.8.2008, p. 1.	
	2.º paso: transmisión de otros datos de carácter personal y de otras informaciones	Legislación nacional Decisión 2006/960/JAI del Consejo («Decisión Marco sueca»).	
Datos de los registros de matriculación de vehículos / Búsqueda automática Prüm de las bases de datos de los registros de matriculación de vehículos (DMV)	Punto de contacto nacional Para las solicitudes recibidas	Decisión 2008/615/JAI del Consejo, artículo 12, DO L 210 de 6.8.2008, p. 1.	
	Para las respuestas/solicitudes emitidas	Ut supra	
Datos del registro del nombre del pasajero	Unidad de Información sobre los Pasajeros	Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, DO L 119 de 4.5.2016, p. 132.	

Sistema de Información de Visados / VIS	Puntos de acceso nacionales centrales	Decisión 2004/512/CE del Consejo, DO L 213 de 15.6.2004, p. 5. Decisión 2008/633/JAI del Consejo, DO L 218 de 13.8.2008, p. 126. Reglamento (CE) n.º 767/2008, *DO L 218 de 13.8.2008.*Lista de las autoridades competentes cuyo personal debidamente autorizado tendrá acceso al sistema para introducir, modificar, suprimir o consultar datos en el Sistema de Información de Visados (VIS) (2016/C 187/04) (DO C 187 de 26.5.2016, p. 4).	

Eurodac	Autoridades nacionales competentes	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.º 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 (refundición), DO L 180 de 29.06.2013, p. 1. *Reglamento (UE) n.º 604/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 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,* DO L 180 de 29.6.2013, p. 31.	

SIA – Sistema de Información Aduanero	Puntos de acceso nacionales	Decisión 2009/917/JAI del Consejo sobre la utilización de tecnología de la información a efectos aduaneros, DO L 323 de 10.12.2009, p. 20.	
Sistema Europeo de Información de Antecedentes Penales / ECRIS	Autoridad Central Nacional	Directiva (UE) 2019/884 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por la que se modifica la Decisión Marco 2009/315/JAI del Consejo en lo que respecta al intercambio de información sobre nacionales de terceros países y al Sistema Europeo de Información de Antecedentes Penales (ECRIS) y por la que se sustituye la Decisión 2009/316/JAI del Consejo, DO L 151 de 7.6.2019, p. 143.	ECRIS - Manual no vinculante para profesionales Disponible en formato electrónico en CIRCABC https://circabc.europa.eu
Red Interinstitucional de Recuperación de Activos de Camden (CARIN)	Organismo de recuperación de activos (ORA)	Decisión 2007/845/JAI del Consejo de 6 de diciembre de 2007 sobre cooperación entre los organismos de recuperación de activos de los Estados miembros en el ámbito del seguimiento y la identificación de productos del delito o de otros bienes relacionados con el delito, DO L 332 de 18.12.2007, p. 103.	Manual de mejores prácticas en la lucha contra los delitos financieros: recopilación de buenos ejemplos de sistemas bien elaborados en los Estados miembros para combatir la delincuencia financiera, 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37.

FIU.NET	Unidades de Información Financiera (UIF)	Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión, DO L 141 de 5.6.2015, p. 73. Ahora las UIF también están reguladas en la Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otros tipos para la prevención, detección, investigación o enjuiciamiento de determinados delitos y por la que se deroga la Decisión 2000/642/JAI del Consejo, DO L 186 de 11.7.2019, p. 122.	Manual de mejores prácticas en la lucha contra los delitos financieros: recopilación de buenos ejemplos de sistemas bien elaborados en los Estados miembros para combatir la delincuencia financiera, 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144 GENVAL 37.

LISTA DE COMPROBACIÓN B: INTERCAMBIO DE INFORMACIÓN CON FINES DE LUCHA CONTRA LOS DELITOS DE TERRORISMO

Sistema de información	**Punto de acceso nacional**	**Base jurídica**	**Manual**
Sistema de Información de Schengen - SIS II	Oficinas Sirene («**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry», solicitud de información complementaria a la entrada nacional)	El acervo de Schengen según se contempla en el artículo 1.2 de la Decisión 1999/435/CE del Consejo, de 20 de mayo de 1999, DO L 239 de 22.9.2000, p. 1. Decisión 2007/533/JAI del Consejo, DO L 205 de 7.8.2007, p. 63. Reglamento (CE) n.º 1986/2006, DO L 381 de 28.12.2006, p. 1. Reglamento (CE) n.º 1987/2006, DO L 381 de 28.12.2006, p. 4.	Versión revisada del catálogo actualizado de recomendaciones y prácticas más idóneas para la correcta aplicación del acervo de Schengen, 13039/11 SCHEVAL 126 SIRIS 79 COMIX 484. Decisión de Ejecución (UE) 2015/219 de la Comisión, de 29 de enero de 2015, por la que se sustituye el anexo de la Decisión de Ejecución 2013/115/UE relativa al Manual Sirene y otras medidas de ejecución para el Sistema de Información de Schengen de segunda generación (SIS II) (comunicada como documento C(2015) 326).

Europol/ Sistema de Información de Europol - Sistema de índice del SIE Ficheros de trabajo de análisis	UNE	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, aplicable desde el 1 de mayo de 2017).	
Interpol I (24 horas al día, 7 días a la semana)	OCN (Oficina Central Nacional)	Reglamento de Interpol sobre el Tratamiento de Datos [III/IRPD/GA/2011(2014)]. Reglamento sobre el Control de la Información y el Acceso a los Ficheros de Interpol, [II.E/RCIA/GA/2004(2009)].	
Búsqueda automática ADN/Prüm de las bases de datos nacionales designadas	Punto de contacto nacional 1er paso: búsqueda automática	Decisión 2008/615/JAI del Consejo, DO L 210 de 6.8.2008, p. 1, artículos 3 y 4.	
	2.º paso: transmisión de otros datos de carácter personal y de otras informaciones	Legislación nacional Decisión 2006/960/JAI del Consejo («Decisión Marco sueca»). DO L 386 de 29.12.2006, p. 89. Corrigenda DO L 75 de 15.3.2007, p. 26.	

Búsqueda automática de impresiones dactilares/Prüm de los AFIS nacionales	Punto de contacto nacional 1er paso: búsqueda automática	Decisión 2008/615/JAI del Consejo, artículo 9, DO L 210 de 6.8.2008, p. 1.	
	2.º paso: transmisión de otros datos de carácter personal y de otras informaciones	Legislación nacional Decisión 2006/960/JAI del Consejo («Decisión Marco sueca»).	
Datos de los registros de matriculación de vehículos / Búsqueda automática Prüm de las bases de datos de los registros de matriculación de vehículos (DMV)	Punto de contacto nacional Para las solicitudes recibidas	Decisión 2008/615/JAI del Consejo, artículo 12, DO L 210 de 6.8.2008, p. 1.	
	Para las respuestas/solicitudes emitidas	Ut supra	
Búsqueda automática ADN/Prüm de las bases de datos nacionales designadas	Punto de contacto nacional 1er paso: búsqueda automática	Decisión 2008/615/JAI del Consejo, DO L 210 de 6.8.2008, p. 1, artículos 3 y 4.	*Guía de aplicación - Intercambio de datos de ADN* 7148/15 DAPIX 40 CRIMORG 25 ENFOPOL 61.
Red Prüm para el suministro de datos personales e información especificada para la prevención de los delitos de terrorismo	Punto de contacto nacional Prüm para la lucha contra el terrorismo	Decisión 2008/615/JAI del Consejo, artículo 16, DO L 210 de 6.8.2008, p. 1.	

Datos del registro del nombre del pasajero	Unidad de Información sobre los Pasajeros	Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, DO L 119 de 4.5.2016, p. 132.	
Sistema de Información de Visados / VIS	Puntos de acceso nacionales centrales	Decisión 2004/512/CE del Consejo, DO L 213 de 15.6.2004, p. 5. Decisión 2008/633/JAI del Consejo, DO L 218 de 13.8.2008, p. 126. Reglamento (CE) n.º 767/2008, DO L 218 de 13.8.2008. Lista de las autoridades competentes cuyo personal debidamente autorizado tendrá acceso al sistema para introducir, modificar, suprimir o consultar datos en el Sistema de Información de Visados (VIS) (2016/C 187/04) (DO C 187 de 26.5.2016, p. 4).	

Eurodac	Autoridades nacionales competentes	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.º 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 (refundición), DO L 180 de 29.06.2013, p. 1. Reglamento (UE) n.º 604/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 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, DO L 180 de 29.6.2013, p. 31.	

Sistema Europeo de Información de Antecedentes Penales / ECRIS	Autoridad Central Nacional	Directiva (UE) 2019/884 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por la que se modifica la Decisión Marco 2009/315/JAI del Consejo en lo que respecta al intercambio de información sobre nacionales de terceros países y al Sistema Europeo de Información de Antecedentes Penales (ECRIS) y por la que se sustituye la Decisión 2009/316/JAI del Consejo, DO L 151 de 7.6.2019, p. 143.	ECRIS - Manual no vinculante para profesionales Disponible en formato electrónico en CIRCABC https://circabc.europa.eu

Sistema centralizado para la identificación de los Estados miembros que poseen información sobre condenas de nacionales de terceros países y apátridas (sistema ECRIS-TCN)	Autoridad Central Nacional	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-TCN) a fin de complementar 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. Directiva (UE) 2019/884 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por la que se modifica la Decisión Marco 2009/315/JAI del Consejo en lo que respecta al intercambio de información sobre nacionales de terceros países y al Sistema Europeo de Información de Antecedentes Penales (ECRIS) y por la que se sustituye la Decisión 2009/316/JAI del Consejo, DO L 151 de 7.6.2019, p. 143.	
Red Interinstitucional de Recuperación de Activos de Camden (CARIN)	Organismo de recuperación de activos (ORA)	Decisión 2007/845/JAI del Consejo de 6 de diciembre de 2007 sobre cooperación entre los organismos de recuperación de activos de los Estados miembros en el ámbito del seguimiento y la identificación de productos del delito o de otros bienes relacionados con el delito, DO L 332 de 18.12.2007, p. 103.	

FIU.NET	Unidades de Información Financiera (UIF)	Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión, DO L 141 de 5.6.2015, p. 73. Ahora las UIF también están reguladas en la Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otros tipos para la prevención, detección, investigación o enjuiciamiento de determinados delitos y por la que se deroga la Decisión 2000/642/JAI del Consejo, DO L 186 de 11.7.2019, p. 122.	

LISTA DE COMPROBACIÓN C: INTERCAMBIO DE INFORMACIÓN CON FINES DE MANTENIMIENTO DEL ORDEN PÚBLICO Y LA SEGURIDAD

Sistema de información	**Punto de acceso nacional**	**Base jurídica**	
Red de puntos de contacto permanentes relativos al orden público	Puntos de contacto nacionales	Acción Común 97/339/JAI, de 26 de mayo de 1997, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, relativa a la cooperación en el ámbito de la seguridad y el orden públicos, artículo 3, letra b), *DO L 147 de 05.06.1997, p. 1.*	
Red Prüm para el suministro de datos no personales y personales para la prevención de delitos y en el mantenimiento del orden público y la seguridad en relación con acontecimientos importantes de dimensión internacional	Punto de contacto nacional Prüm / acontecimientos importantes	Decisión 2008/615/JAI del Consejo, artículo 15, DO L 210 de 6.8.2008, p. 1. Legislación nacional	

Red de puntos nacionales de información futbolística	Puntos nacionales de información futbolística / PNIF	Decisión (2002/348/JAI) del Consejo, de 25 de abril de 2002, relativa a la seguridad en los partidos de fútbol de dimensión internacional, DO L 121 de 8.5.2002, p. 1. Decisión (2007/412/JAI) del Consejo, de 12 de junio de 2007, por la que se modifica la Decisión 2002/348/JAI relativa a la seguridad en los partidos de fútbol de dimensión internacional, DO L 155 de 15.6.2007, p. 76.	Recomendación (2007/C 314/07) del Consejo, de 6 de diciembre de 2007, sobre un Manual para las autoridades de policía y seguridad relativo a la cooperación en grandes acontecimientos de dimensión internacional. DO C 314 de 22.12.2007, p. 4. Resolución del Consejo, de 3 de junio de 2010, relativa a un manual actualizado de recomendaciones para la cooperación policial internacional y de medidas de prevención y lucha contra la violencia y los desórdenes relacionados con los partidos de fútbol de dimensión internacional en los que se vea afectado al menos un Estado miembro. DO C 165 de 24.6.2010, p. 1.

Red de Protección de Personalidades	Puntos de acceso nacionales	Decisión 2009/796/JAI del Consejo, de 4 de junio de 2009, por la que se modifica la Decisión 2002/956/JAI relativa a la creación de una red europea de protección de personalidades, DO L 283 de 30.10.2009, p. 62.	Manual de la Red europea de protección de personalidades 10478/13 ENFOPOL 173.
Centros de Cooperación Policial y Aduanera	CCPA	Acuerdos bilaterales	

PARTE II: INFORMACIÓN GENERAL

1. CAUCES DE CONTACTO[3]

1.1. PUC - Punto único de contacto

Numerosos puntos de contacto nacionales

Los Estados miembros, tanto en calidad de Estado solicitado como de Estado solicitante, hacen frente al incremento del flujo transfronterizo de información mejorando la eficacia de sus estructuras y redes operativas, tanto a nivel nacional como europeo. Varios de los instrumentos jurídicos de la UE relativos a la cooperación policial transfronteriza instan a la creación de autoridades, órganos o servicios competentes específicos o de puntos de contacto nacionales (PCN). La policía, las aduanas u otras autoridades competentes autorizadas por el Derecho nacional deben intercambiar información entre sí mediante estos puntos de contacto nacionales designados que, dentro de un Estado miembro determinado, pueden pertenecer a diferentes departamentos de las fuerzas de seguridad a aún a diferentes ministerios. Con el fin de ofrecer una visión general, en la Parte III del presente documento figuran unas listas de puntos de contacto nacionales específicos para el intercambio de información en el nivel de la UE en el ámbito del intercambio de datos relativo a la acción policial, que la SGC emite y actualiza periódicamente.

Principio de disponibilidad - Decisión Marco sueca

El intercambio de información e inteligencia de tipo policial[4] y de carácter transfronterizo debe cumplir las condiciones que se derivan del «principio de disponibilidad» aplicado por la «Decisión Marco sueca». Ello tiene como consecuencia:

- que un agente de policía de un Estado miembro que necesite información con el fin de desempeñar su misión puede obtenerla de otro,

- que las autoridades policiales del Estado miembro que posea esta información la pondrán a disposición con los fines declarados, teniendo en cuenta las necesidades de las investigaciones en curso en dicho Estado miembro, y

---

3 Los órganos que intervienen en el intercambio de información policial.

4 A los efectos del presente manual, se entenderá por «policial» la prevención, detección o investigación de delitos de terrorismo, tal como se definen en la Directiva (UE) 2017/541, o de delitos graves, tal como se definen en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI relativa a la orden de detención europea, cuando estén tipificados en la legislación nacional con una pena o una medida de seguridad privativas de libertad de un periodo máximo no inferior a tres años.

- que una vez que haya información policial disponible en un Estado miembro, esta será compartida de modo transfronterizo en las mismas condiciones que rigen la puesta en común de información en el ámbito nacional, lo que implica que las normas aplicadas en un caso transfronterizo no sean más estrictas que las que se apliquen a los intercambios de datos en el ámbito nacional («principio de acceso equivalente»).

Punto único de contacto (PUC)

La combinación de los estrictos requisitos de la Decisión Marco sueca y de la existencia de estrategias nacionales diferentes para gestionar las diferentes iniciativas de intercambio de información exige, en el ámbito nacional, un planteamiento más sencillo y uniforme, con el fin de conseguir que todas las solicitudes de información entre organismos policiales en la UE sean atendidos con eficacia y eficiencia.

Las Conclusiones del Consejo sobre el Modelo Europeo para el Intercambio de Información (EIXM)[5], adoptadas en junio de 2013, reconocían el potencial del punto único de contacto para el intercambio de información dentro de cada Estado miembro para contribuir a racionalizar el proceso en un entorno jurídico y operativo cada vez más complejo.

Casi todos los Estados miembros han aplicado la política de conseguir el máximo intercambio de información posible mediante un punto único de contacto, si bien la comprensión del concepto de PUC parece diferir de un Estado miembro a otro. Las directrices sobre los PUC[6] indican de qué manera pueden estructurarse los PUC para aprovechar al máximo sus recursos, evitar las duplicaciones y hacer la cooperación con otros Estados miembros más eficiente, rápida y transparente.

De estas directrices, los Estados miembros deberían seleccionar la solución apropiada a su situación en vista del objetivo común y acordado de mejorar la cooperación internacional y estudiar fórmulas adecuadas para informar a los demás Estados miembros de la solución elegida con vistas al intercambio de las mejores prácticas.

---

5 Conclusiones del Consejo tras la comunicación de la Comisión sobre el Modelo Europeo para el Intercambio de Información (EIXM), 9811/13 JAI 400 DAPIX 82 CRIMORG 76 ENFOCUSTOM 88 ENFOPOL 146.

6 «Proyecto de directrices sobre un punto único de contacto para el intercambio internacional de información policial», 10492/14 DAPIX 75 ENFOPOL 157 y 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1.

Idealmente, el PUC:

- tendrá acceso a la más amplia variedad de bases de datos policiales pertinentes, tanto nacionales como europeas e internacionales, con el fin de efectuar expeditivamente el intercambio directo de información entre las autoridades nacionales competentes;

- acogerá las unidades nacionales de Sirene, Europol e Interpol;

- acogerá el punto de contacto para los agentes de enlace, los puntos de contacto designados en virtud de las Decisiones «Prüm» y «sueca» y, en su caso, los puntos de contacto de las oficinas regionales y bilaterales;

- estará constituido en un entorno de trabajo seguro y tendrá una plantilla suficiente y adecuada, con inclusión de servicios de interpretación o traducción, para poder funcionar veinticuatro horas al día y siete días a la semana. En la medida de lo posible, todo el personal debería estar formado, equipado y dotado de mandato para hacer frente a todos los tipos de tareas dentro del PUC. Cuando esto no sea posible, debería garantizarse que unos funcionarios de guardia puedan hacerse cargo de todas las tareas veinticuatro horas al día y siete días a la semana;

- será una organización compuesta de varios organismos que consta de personal procedente de distintos servicios o ministerios, que incluyen la policía judicial, las guardias fronterizas, las aduanas y las autoridades judiciales.

Estructura típica de la oficina de un PUC (punto único de contacto) nacional

La Unidad Central de Cooperación Policial Operativa,

Plataforma de intercambio de información

*La S.C.C.O.Pol es una estructura **interministerial**, compuesta por 67 agentes de policía, gendarmes y agentes de aduanas. Los magistrados del Servicio de Cooperación Internacional en Materia Penal (B.E.P.I.) del Ministerio de Justicia también prestan, en el mismo local, un servicio básico de validación de las solicitudes francesas de expedición de órdenes de detención europeas y de registro en el archivo nacional de personas buscadas de las solicitudes de detención y notificaciones rojas extranjeras.*

*Para garantizar la necesaria **transversalidad** de los tres canales de cooperación, en agosto de 2004 fue designado, en la S.C.C.O.Pol, un punto central de contacto (P.C.C.). Su principal función consiste en asistir a los servicios policiales franceses en la elección de la mejor herramienta de cooperación policial según la naturaleza y complejidad de la investigación en curso. Comprueba la legalidad de la solicitud, realiza los primeros cotejos y la redirige al canal de cooperación más adecuado en función de la solicitud de los investigadores. Únicamente las solicitudes relativas a una descripción de Schengen son de competencia exclusiva de S.I.R.E.N.E. Francia.*

*Como resultado de una puesta en común exitosa de los recursos, la S.C.C.O.Pol trata, **las veinticuatro horas del día**, casi **350 000 mensajes al año**, en una **plataforma segura única**, con una plantilla reducida.*

La jurisdicción de la S.C.C.O.Pol, que abarca diversos canales, le permite hacerse cargo de la representación de Francia en los grupos europeos (SIS/VIS, SIS/Sirene, jefes de UNE) o en los grupos de Interpol (reunión de funcionarios de contacto de Interpol, grupos de notificaciones) y aportar un punto de vista operativo pertinente a la unidad de la DRI que es responsable, en Francia, de la observación de los órganos de gestión de Interpol y de Europol.

1.2. Oficinas Sirene

Las oficinas Sirene son cruciales para las operaciones del Sistema de Información de Schengen y para el intercambio de información. En cada Estado miembro se ha creado una oficina permanente de Sirene («**S**upplementary **I**nformation **Re**quest at the **N**ational **E**ntry», solicitud de información complementaria a la entrada nacional) como parte del acervo de Schengen[7], constituida como autoridad designada responsable, a nivel central, de la sección nacional del Sistema de Información de Schengen (SIS II). Son el punto de contacto de las oficinas Sirene de otras partes contratantes y el enlace con las autoridades y agencias nacionales. El SIS II cuenta con un sistema de respuesta positiva o negativa basada en búsquedas. Durante las veinticuatro horas del día, las oficinas intercambian datos en relación con las descripciones SIS II[8], (una descripción es una serie de datos que permiten a las autoridades identificar personas u objetos con vistas a tomar las medidas oportunas).

Por «información complementaria» se entiende la información no almacenada en el SIS II pero relacionada con las descripciones del SIS II, que se intercambiará, bilateral o multilateralmente, mediante formularios:

i) a fin de que los Estados miembros puedan consultarse o informarse entre sí al introducir una descripción;

ii) tras la obtención de una respuesta positiva, a fin de poder emprender la acción adecuada;

iii) cuando no pueda realizarse la acción requerida;

iv) al tratar de la calidad de los datos del SIS II;

v) al tratar de la compatibilidad y prioridad de las descripciones;

vi) y al tratar del ejercicio del derecho de acceso.

---

7 Véase el Convenio de aplicación del Acuerdo de Schengen, DO L 239 de 22.9.2000.

8 Véase la Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), DO L 205 de 7.8.2007, p. 63.

La información debe intercambiarse de conformidad con las disposiciones del Manual Sirene[9] y a través de la infraestructura de comunicación[10]. El SIS II[11] posee funciones mejoradas en comparación con su predecesor, como la opción de introducir impresiones dactilares y fotografías, nuevas categorías de objetos (aeronaves, embarcaciones, contenedores, medios de pago robados) o la posibilidad de que el responsable de la alerta vincule diversas alertas. El SIS II contiene copias de las órdenes de detención europeas directamente asociadas a las alertas sobre las personas de que se trate.

Las oficinas Sirene facilitan la cooperación en materia policial y pueden desempeñar también un papel en el intercambio de información fuera del ámbito de SIS II, en virtud de las disposiciones anteriormente contenidas en los artículos 39 y 46 del CAS, que han sido sustituidas por la **«Decisión Marco sueca».** El artículo 12, apartado 1, de la «Decisión Marco sueca» establece que las disposiciones del artículo 39, apartados 1, 2 y 3, y del artículo 46 del Convenio de Aplicación del Acuerdo de Schengen (CAS), en la medida en que se refieren al intercambio de información e inteligencia a efectos de la realización de investigaciones y de operaciones de inteligencia criminal previstas en la Decisión Marco, quedan sustituidas por las disposiciones de la Decisión Marco.

1.3. La Unidad Nacional de Europol (UNE)

Cada Estado miembro tiene una Unidad Nacional de Europol (UNE) designada, que es el órgano de enlace entre Europol y las autoridades nacionales competentes. Los funcionarios de enlace de la UNE destinados a Europol deben constituir un enlace permanente entre la sede de Europol en La Haya y las UNE de los 28 Estados miembros. Europol acoge asimismo a funcionarios de enlace de diez países y organizaciones no pertenecientes a la UE. La red se apoya en unos canales de comunicación seguros provistos por Europol.

---

9 Decisión de Ejecución de la Comisión, de 26 de febrero de 2013, relativa al Manual Sirene y otras medidas de ejecución para el Sistema de Información de Schengen de segunda generación (SIS II) (comunicada como documento C(2013) 1043**),** DO L 71 de 14.3.2013, p. 1.

10 Debido a la clausura de la red de correo SISnet, ahora las oficinas Sirene pueden utilizar el servicio de correo sTESTA. Puede haber otros intercambios de información a través de la red sTESTA, SIENA o los canales de comunicación I-24/7.

11 Informe de la Comisión al Parlamento Europeo y al Consejo sobre la evaluación del Sistema de Información de Schengen de segunda generación (SIS II), de conformidad con el artículo 24, apartado 5, el artículo 43, apartado 3, y el artículo 50, apartado 5, del Reglamento (CE) n.º 1987/2006 y con el artículo 59, apartado 3, y el artículo 66, apartado 5, de la Decisión 2007/533/JAI, 15810/16 SIRIS 175 COMIX 860.

Europol[12] apoya a las autoridades policiales de los Estados miembros en la prevención y lucha contra la delincuencia organizada, la delincuencia internacional grave y el terrorismo cuando afecta a dos o más Estados miembros. Para recopilar, almacenar, tratar y analizar datos personales e intercambiar información e inteligencia, Europol depende de la aportación de datos por parte de los Estados miembros. El Reglamento Europol establece las distintas funciones en relación con la información así como las normas relativas al uso de los datos y a su intercambio con terceros, conforme a un estricto régimen de protección y seguridad de los datos.

1.4. Las Oficinas Centrales Nacionales (OCN) de Interpol

Las **Oficinas Centrales Nacionales (OCN)** en las sedes centrales de las policías nacionales desempeñan un papel fundamental en relación con el tratamiento de los datos que facilitan sus países al Sistema de Información de Interpol. Tienen derecho a acceder directamente al sistema, lo que incluye:

- la grabación, actualización y borrado de datos directamente en las bases de datos policiales de la organización, así como la creación de enlaces entre datos;
- la consulta directa de estas bases de datos;
- el uso de las notificaciones y circulares de Interpol para la transmisión de las solicitudes de cooperación y las descripciones internacionales.

Las OCN pueden buscar y cotejar datos rápidamente con un acceso directo, en todo momento y a todas horas, a las bases de datos que contienen información sobre sospechosos de terrorismo, personas buscadas, impresiones dactilares, perfiles de ADN, documentos de viaje perdidos o sustraídos, vehículos de motor robados, obras de arte robadas, etc.

[12] 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, aplicable desde el 1 de mayo de 2017).

En la medida de lo posible, las OCN deben permitir a las autoridades instructoras de sus países que intervienen en la cooperación policial internacional acceder al Sistema de Información de Interpol. Las OCN controlan el nivel de acceso a los servicios de Interpol que tienen otros usuarios autorizados de sus países, y pueden pedir que se les informa de las consultas hechas por otros países a sus bases de datos.

1.5. Puntos de contacto nacionales Prüm

Las «decisiones de Prüm»[13] abrieron una nueva dimensión transfronteriza de la lucha contra la delincuencia al proveer un acceso común transfronterizo a las bases de datos ADN nacionales designadas, a los sistemas automáticos de identificación dactilar (SAID) y a las bases de datos de los registros de matriculación de vehículos (DMV). Con el fin de facilitar datos, se designa un punto de contacto nacional (PCN) específico para cada tipo de intercambio de datos en cada Estado miembro participante[14]. Unas disposiciones sobre protección de datos y sobre seguridad de los datos adaptadas tienen en cuenta, en particular, la especificidad del acceso en línea a estas bases de datos. El suministro de datos personales exige un nivel suficiente de protección y seguridad de los datos, ensayada en común y convenida entre los Estados miembros antes de iniciar el intercambio de datos.

1.5.1. PCN Prüm - ADN e impresiones dactilares

En el caso de los datos de ADN e impresiones dactilares, la comparación automática de los índices de referencia biométricos se basa en un sistema de consultas de coincidencias. Los índices de referencia no permiten identificar inmediatamente al interesado. En caso de coincidencia, el PCN del Estado miembro que realice la consulta podrá, por lo tanto, pedir más datos personales específicos. El suministro de estos datos suplementario debe solicitarse mediante procedimientos de asistencia mutua, incluidos los adoptados con arreglo a la «Decisión Marco sueca», y se rige por el Derecho nacional, incluidas las normas de asistencia jurídica, del Estado miembro requerido.

---

13 Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza (DO L 210 de 6.8.2008, p. 1); Decisión 2008/616/JAI del Consejo, de 23 de junio de 2008, relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza (DO L 210 de 6.8.2008, p. 12).

14 5010/15 JAI 1 DAPIX 1 ENFOPOL 1 CRIMORG 1.

1.5.1.1. Directrices sobre las mejores prácticas para las consultas de impresiones dactilares

Al utilizar el instrumento de búsqueda automática de impresiones dactilares de Prüm, el Estado miembro requirente debe seguir las recomendaciones que figuran en el documento «Buenas prácticas para consultar las bases de datos de los Estados miembros» (14885/1/08 REV 1). Este documento reconoce la limitación de las capacidades de búsqueda de las **bases de datos dactiloscópicas** y recomienda que se promueva, a nivel operativo, las siguientes prácticas:

- El consultar o no las bases de datos sobre impresiones dactilares de los Estados miembros, así como el orden en el que dichas consultas se realizan y repiten, son decisiones de investigación tomadas caso por caso y que no deben predeterminarse sistemáticamente.

- En principio, no deben consultarse las bases de datos de impresiones dactilares de otros Estados miembros mientras no se hayan consultado las propias bases de datos del Estado requirente.

- A la hora de decidir si se consultan las bases de datos de uno o más Estados miembros, debe tenerse en cuenta, en particular lo siguiente:

  – la gravedad del caso;

  – o las líneas de investigación existentes, en particular información que apunte a un Estado miembro o grupo de Estados miembros;

  – o los requisitos específicos de la investigación.

- No deben realizarse consultas generales mientras no se hayan agotado las buenas prácticas de los puntos 1, 2 y 3.

Ejemplos de intercambio automático de datos con arreglo a las Decisiones del Consejo de Prüm

En 2011, durante la instrucción de un delito de homicidio, se introdujo material genético en la base de datos de ADN nacional checa. La instrucción se estaba llevando a cabo contra un sospechoso que había huido al extranjero. El material genético se obtuvo a partir de una colilla de cigarrillo dentro de un cenicero, en el apartamento en el que se cometió el crimen. Al consultar la base de datos de ADN austriaca en 2014, se descubrió que en Austria se había tratado el mismo perfil. Los PUC de los dos países intercambiaron más datos personales por medio de la cooperación policial. Posteriormente, se estableció un contacto con el departamento de justicia penal y se le solicitó la entrega del sospechoso a la República Checa, mediante asistencia judicial en materia penal, para la acción penal.

En 2005, durante la instrucción de un caso de robo, se introdujo un perfil de ADN en la base de datos de ADN nacional checa. En 2014 se identificó a un sospechoso tras consultar la base de datos de ADN austriaca. Se solicitó a la parte austriaca que remitiese una fotografía reciente y otros datos personales por medio de los PUC.

1.5.2. PCN Prüm - datos del registro de matriculación de vehículos (DMV)

Con respecto a DMV, las búsquedas pueden hacerse con el número completo del bastidor en un Estado miembro participante o en todos ellos, o con un número de matrícula completo en un Estado miembro en particular. Los PCN designados para las peticiones tanto recibidas como enviadas intercambiarán la información entre sí. Los Estados miembros se otorgarán unos a otros el acceso en línea a DMV para

a) los datos de los propietarios o usuarios, y

b) los datos de los vehículos.

Los Estados miembros utilizar una versión de la aplicación informática EUCARIS (sistema europeo de información sobre vehículos y permisos de conducción) concebida especialmente para los fines de Prüm de realizar estas consultas. Las consultas de DMV difieren de las del ADN y las impresiones dactilares en que, en caso de coincidencia, presentan tanto datos personales como índices de referencia. Como ocurre con otras búsquedas automáticas, se entiende que la oferta de datos personales está sujeta al nivel adecuado de protección de datos que apliquen los Estados miembros receptores.

1.5.3. PCN de Prüm para la prevención del terrorismo

Bien a petición de parte o por propia iniciativa, los PCN designados pueden intercambiar información sobre personas sospechosas de cometer delitos de terrorismo. Los datos incluirán el apellido, nombre de pila, fecha y lugar de nacimiento del sospechoso y una descripción de las circunstancias que permiten creer que el interesado vaya a cometer infracciones penales relacionadas con actividades terroristas.

El Estado miembro transmisor podrá establecer condiciones, con arreglo a su Derecho interno, respecto de la utilización de dichos datos e informaciones por el Estado miembro receptor, que estará obligado por dichas condiciones.

1.5.4. PCN Prüm para grandes acontecimientos

Los Estados miembros en los que se celebren grandes acontecimientos de dimensión internacional deben garantizar la seguridad del acto de que se trate tanto desde la perspectiva del orden público como desde una perspectiva antiterrorista. Según la naturaleza del acontecimiento (política, deportiva, social, cultural u otra), una de las perspectivas puede ser más importante que la otra. No obstante, tienen que considerarse los dos aspectos, aunque quizá cada uno sea atendido por una autoridad diferente. Se presta una atención particular al fenómeno de los infractores violentos en desplazamiento, en particular en relación con los partidos de fútbol internacionales.

Con el fin de impedir las infracciones penales y mantener el orden público y la seguridad en relación con los grandes acontecimientos y agrupaciones de masas semejantes (sean de carácter político, deportivo, social, cultural u otros), las catástrofes y los accidentes graves con incidencia transfronteriza, los PCN designados se facilitan entre sí, a petición de parte o por iniciativa propia

- datos no personales, o
- datos personales, si por sentencias firmes u otras circunstancias, existe motivo para pensar que los interesados van a cometer infracciones penales en los acontecimientos, o presentan una amenaza al orden público y a la seguridad.

Los datos de carácter personal solo podrán ser tratados para los fines arriba mencionados y en relación con el acontecimiento concreto para el que se hayan comunicado. Los datos suministrados deben suprimirse inmediatamente una vez conseguidos estos propósitos, y en cualquier caso al cabo de un año a más tardar. La información se facilita con arreglo al Derecho interno del Estado miembro que la facilita.

1.5.4.1. Manual relativo a la cooperación en grandes acontecimientos de dimensión internacional[15]

Este manual contiene unas directrices y sugerencias para las autoridades policiales que tengan encomendada la tarea de garantizar la seguridad en grandes acontecimientos como los Juegos Olímpicos u otros actos deportivos o sociales importantes o reuniones políticas de alto nivel.

El manual, que se modifica y adapta constantemente en función del desarrollo de las mejores prácticas, contiene orientación sobre la gestión de la información y la gestión de los acontecimientos, así como sobre la evaluación relativa al acontecimiento y la evaluación estratégica. Los formularios normalizados anexos se refieren a:

- las solicitudes a los funcionarios de enlace;
- el análisis de riesgos sobre posibles manifestantes y otras agrupaciones;
- el intercambio de información sobre individuos o grupos que suponen una amenaza terrorista;
- una lista de documentos de consulta;
- un cuadro que contiene puntos de contacto permanentes relativos al orden público.

1.6. Punto nacional (policial) de información futbolística (PNIF)[16]

Además del PCN Prüm para los acontecimientos importantes y con atención particular a los partidos de fútbol internacionales, en cada Estado miembro existe un punto nacional de información futbolística (PNIF) con la función de intercambiar la información pertinente y desarrollar una cooperación policial transfronteriza. La información táctica, estratégica y operativa puede ser aprovechada por el propio PNIF o remitida a las autoridades o servicios policiales correspondientes.

Es el PNIF el que coordina y, en su caso, organiza los contactos entre los servicios policiales de los diferentes países implicados en un acontecimiento. El sitio internet de los NFIP alojado en el CIV (www.nfip.eu) difunde la información y la asesoría sobre las posibilidades jurídicas y otras en relación con la seguridad y la prevención en relación con los partidos de fútbol.

---

15 Recomendación (2007/C 314/02) del Consejo, de 6 de diciembre de 2007, sobre un Manual para las autoridades de policía y seguridad relativo a la cooperación en grandes acontecimientos de dimensión internacional (DO C 314 de 22.12.2007, p. 4).

16 Decisión 2002/348/JAI del Consejo, de 25 de abril de 2002, relativa a la seguridad en los partidos de fútbol de dimensión internacional (DO L 121 de 8.5.2002, p. 1).

El PNIF coordina el tratamiento de la información relativa a los hinchas de alto riesgo con el fin de preparar y adoptar las medidas adecuadas con el fin de mantener el orden público cuando se celebra un acontecimiento futbolístico. Dicha información incluye, en especial, los detalles de individuos que supongan real o potencialmente una amenaza para el orden público y la seguridad. Debe intercambiarse información sobre los formularios[17] que figuran en el apéndice al manual sobre fútbol.

1.6.1. Manual para el fútbol[18]

El Manual para el fútbol, que figura anejo a la Resolución 2006/C 322/01 del Consejo, presenta ejemplos de modos de cooperación policial en el ámbito internacional para la prevención y el control de la violencia y los disturbios relacionados con los partidos de fútbol. El contenido consta, en particular, de unas recomendaciones relativas a:

- la gestión de la información por parte de servicios policiales;
- la organización de la cooperación entre las fuerzas de policía;
- una lista de comprobación para la política de medios y la estrategia de comunicación (policía/autoridades).

1.7. Centros de Cooperación Policial y Aduanera (CCPA)

Los CCPA se crean en virtud de acuerdos bilaterales o multilaterales, de conformidad con el artículo 39.4 del Convenio de aplicación del Acuerdo de Schengen (CAS). En esos acuerdos, las partes contratantes definen las bases de su cooperación transfronteriza, que incluyen los cometidos, el marco jurídico y los procedimientos para la creación y funcionamiento de los centros. Los CCPA reúnen personal de los países limítrofes y están estrechamente ligados a los organismos nacionales responsables de la cooperación internacional (PCN, OCN Interpol, UNE, oficinas Sirene).

---

17 Decisión 2007/412/JAI del Consejo, de 12 de junio de 2007, por la que se modifica la Decisión 2002/348/JAI relativa a la seguridad en los partidos de fútbol de dimensión internacional (DO L 155 de 15.6.2007, p. 76).

18 Resolución del Consejo relativa al Manual actualizado de recomendaciones para la cooperación policial internacional y de medidas de prevención y lucha contra la violencia y los desórdenes relacionados con los partidos de fútbol de dimensión internacional en los que se vea afectado al menos un Estado miembro («Manual para el fútbol de la UE»), 2016/C 444/01 (DO C 444 de 29.11.2016, p. 1).

Los CCPA ofrecen asesoría y apoyo no operativo a los servicios operativos nacionales policiales, aduaneros y otros en la región fronteriza donde están situados. La plantilla de los CCPA tiene por misión facilitar rápidamente la información solicitada en virtud de la Decisión 2006/960/JAI del Consejo («Decisión Marco sueca»).

A finales de 2016, ocho de los 59 CCPA existentes estaban vinculados a SIENA, la aplicación de la red de intercambio seguro de información de Europol. El intercambio de información a través de estos centros se refiere principalmente a delitos menores o de gravedad media, a flujos de inmigración ilegal o a desórdenes públicos. Dicha información puede incluir la identificación de conductores o la verificación de la adecuación y autenticidad de documentos de identidad y viaje.

Las Partes contratantes pueden decidir de común acuerdo convertir un CCPA en un centro regional de coordinación de operaciones al servicio de todos los servicios afectados, en particular en caso de incidentes de alcance regional (catástrofes naturales) o de acontecimientos de gran importancia (Juegos Olímpicos, Campeonato Mundial de Fútbol, etc.).

Si un CCPA recibe información que compete a una unidad central nacional, debe remitir inmediatamente esa información al PUC o unidad central. En caso de que un CCPA reciba información de interés evidente para Europol, podrá transmitir esta información a la UNE localizada en el PUC, que la trasladará a la propia Europol.

Ejemplo de intercambio de información por medio de un CCPA

EPICC («Euregio Police Information and Cooperation Centre») es la abreviatura del CCPA de Heerlen.

Fue creado ad hoc (sin instrumento jurídico particular) en 2005 por iniciativa del «NeBeDeAgPol», una asociación de jefes de Policía de la eurorregión Mosa-Rin, situada en la región fronteriza entre los Países Bajos, Bélgica y Alemania, una de las zonas fronterizas con mayor densidad de población de la Unión Europea.

En este CCPA colaboran, en una plataforma única, alrededor de treinta agentes de Policía belgas, alemanes y neerlandeses.

Estos agentes disponen de acceso in situ a la mayor parte del contenido de las bases de datos de sus respetivos países. Ello les permite proveer –dentro de un plazo muy breve– respuestas precisas, completas y fiables a las solicitudes de información de la Policía relativas a BE, DE o NL. El intercambio de información entre las tres delegaciones del EPICC se hace por medio de la aplicación de Europol «SIENA».

El EPICC recopila y analiza la información policial disponible en la región fronteriza con el fin de detectar, describir y seguir los problemas de seguridad en la frontera (nuevos fenómenos o modi operandi, grupos de delincuentes que actúan en la región fronteriza, hechos o personas que requieren atención particular, etc.).

Gracias a su pericia especial y a su composición mixta, el CCPA de Heerlen puede prestar un apoyo eficaz durante la preparación y ejecución de las operaciones, investigaciones o medidas de seguridad transfronterizas.

1.8. Funcionarios de enlace

El Convenio de aplicación del Acuerdo de Schengen (CAS), en su artículo 47, dispone que los Estados miembros «podrán suscribir acuerdos bilaterales que permitan el destino provisional, por un período determinado o indeterminado, de funcionarios de enlace de un Estado [miembro] en servicios de policía de otro Estado [miembro]». La función de los funcionarios de enlace consiste en establecer y mantener contactos directos para favorecer y acelerar la cooperación con el fin de luchar contra la delincuencia, en particular brindando asistencia. Los funcionarios de enlace no están habilitados para ejecutar medidas policiales de modo autónomo. Aseguran una cooperación rápida y eficaz, basada en el contacto personal y la confianza mutua:

- facilitando y acelerando la recopilación e intercambio de información;
- ejecutando las peticiones de cooperación policial y judicial en materia penal;
- organizando y garantizando las operaciones transfronterizas.

Los funcionarios de enlace pueden ser destinados a otros Estados miembros, terceros países o agencias de la UE u organizaciones internacionales. El Compendio[19] sobre funcionarios de enlace policiales, que la Secretaría General del Consejo actualiza cada año, explica el trabajo y las funciones de los funcionarios de enlace y contiene listas de funcionarios de enlace con los datos de contacto.

A partir de las experiencias pasadas y presentes en los diferentes países de acogida, y con el fin de poner en común, en mayor medida, las actividades de los Estados miembros en relación con los terceros países, tanto en cuanto el trabajo de los funcionarios de enlace como en cuanto a la cooperación técnica, se han descrito algunas buenas prácticas, que se exponen en el Compendio. Se sugiere a los funcionarios de enlace de los Estados miembros y a sus autoridades correspondientes que apliquen dichas prácticas cuando sea oportuno.

---

[19] '*Update of the Compendium on law enforcement liaison officers (2018)*', («Actualización del Compendio sobre funcionarios de enlace policiales (2018)», solo en lengua inglesa), 10095/1/18 REV 1 ENFOPOL 397 JAIEX 84 COMIX 422.

Ejemplos típicos de intercambio de información entre funcionarios de enlace

- *Se puede encomendar a los funcionarios de enlace la función de mantener el contacto con el fin de establecer una cooperación directa en casos particulares como la delincuencia relacionada con las drogas.*
- *Los funcionarios de enlace pueden facilitar información específica sobre las normas y la legislación nacionales relativas a la cooperación policial internacional o a la asistencia judicial en materia penal.*
- *Los funcionarios de enlace, en algunos casos, mantienen listas actualizadas de autoridades responsables de su Estado miembro.*
- *En algunos Estados miembros, también se ha encomendado a los funcionarios de enlace que atiendan las solicitudes de cooperación en virtud del artículo 17 de la Decisión Prüm (Operaciones conjuntas). Por ejemplo, la República Checa pidió al funcionario de enlace danés en Europol que trasladara una petición a Dinamarca de destinar cuatro agentes de policía daneses para asistir en un caso que afectaba a los dos Estados miembros.*

1.9. Organismos de recuperación de activos (ORA) de los Estados miembros

Un delito financiero abarca una amplia selección de actividades tales como la falsificación, la corrupción y el fraude (p. ej. fraude con tarjeta de crédito, préstamo hipotecario, fraude médico o de valores, cohecho o malversación, blanqueo de capitales, usurpación de identidad y evasión fiscal). Se consiguió una mayor cooperación mediante una colaboración transfronteriza más estrecha entre organismos de recuperación de activos (ORA), Unidades de Información Financiera (UIF) y autoridades policiales y aduaneras.[20]

Después de la adopción de la Decisión 2007/845/JAI del Consejo, de 6 de diciembre de 2007, sobre cooperación entre los organismos de recuperación de activos de los Estados miembros en el ámbito del seguimiento y la identificación de productos del delito o de otros bienes relacionados con el delito[21], desde entonces todos los Estados miembros crearon y designaron organismo de recuperación de activos (ORA). Estas unidades especializadas se convirtieron en una red unida de especialistas capaces de intercambiar directamente información sobre asuntos relativos a la recuperación de patrimonio a través del sistema SIENA. Bajo los auspicios de la Comisión Europea y Europol, la red de ORA facilita la cooperación entre los organismos de recuperación de activos de los Estados miembros, así como el debate estratégico y el intercambio de mejores prácticas. La Oficina de Activos de Origen Delictivo (ECAB) de Europol actúa como punto central para la recuperación de activos dentro de la UE.

Las disposiciones que establece la Directiva 2014/42/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, sobre el embargo y el decomiso de los instrumentos y del producto del delito en la Unión Europea[22] aumentarán la eficacia de la cooperación entre los organismos de recuperación de activos de la Unión Europea. Los Estados miembros tienen que transponer la Directiva antes del 4 de octubre de 2016.

---

20 Manual de mejores prácticas en la lucha contra los delitos financieros: Una recopilación de buenos ejemplos de sistemas bien desarrollados en los Estados miembros de lucha contra delitos financieros, 9741/13 JAI 393 COSI 59 CRIMORG 75 ENFOPOL 144.

21 Decisión 2007/845/JAI del Consejo, de 6 de diciembre de 2007, sobre cooperación entre los organismos de recuperación de activos de los Estados miembros en el ámbito del seguimiento y la identificación de productos del delito o de otros bienes relacionados con el delito (DO L 332 de 18.12.2007, p. 103).

22 Directiva 2014/42/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, sobre el embargo y el decomiso de los instrumentos y del producto del delito en la Unión Europea (DO L 127 de 29.4.2014, p. 39).

La **Red Interinstitucional de Recuperación de Activos de Camden (CARIN)**, creada en 2004 para apoyar la identificación, el embargo, la incautación y la confiscación transfronterizos de propiedades relacionados con delitos, intensifica el intercambio mutuo de información relativa a diferentes planteamientos nacionales extendidos mas allá de la UE.

Desde 2015, la red CARIN engloba a profesionales de 53 jurisdicciones y 9 organizaciones internacionales que sirven de puntos de contacto a fin de agilizar el intercambio de información transfronterizo, previa petición o de manera espontánea. Los ORA nacionales cooperan entre sí, o con otras autoridades, a fin de facilitar el seguimiento y la identificación de productos del delito. Aunque todos los Estados miembros han establecido un ORA, existen grandes diferencias entre Estados miembros en términos de estructura organizativa, recursos y actividades.

La información intercambiada puede utilizarse con arreglo a las disposiciones de protección de datos de los Estados miembros receptores y está sujeta a las mismas normas de protección de datos que si hubiera sido recogida en el Estado miembro receptor. Ha de fomentarse el intercambio espontáneo de información con arreglo a la presente Decisión, aplicando los procedimientos y plazos previstos en la denominada «Decisión Marco sueca».

1.10. Blanqueo de capitales - Cooperación entre Unidades de Información Financiera (UIF)[23][24]

Toda información pertinente sobre cualquier hecho que pueda ser un indicio de blanqueo de capitales o financiación del terrorismo debe remitirse a las Unidades de Información Financiera (UIF). Las UIF analizan la información recibida caso por caso con el objeto de establecer vínculos entre las transacciones sospechosas y la actividad delictiva subyacente para prevenir y combatir el blanqueo de capitales y la financiación del terrorismo. Las UIF actúan como unidad nacional central para recibir y analizar la información y transmitir los resultados de sus análisis a las autoridades competentes. Las UIF, que gozan de autonomía e independencia operativa, desempeñan sus funciones libremente, por ejemplo, toman decisiones autónomas sobre el análisis, la solicitud y la difusión de información específica.

---

23 Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo de 20 de junio de 2019 por la que se establecen normas destinadas a facilitar el uso de información financiera y de otros tipos para la prevención, detección, investigación o enjuiciamiento de infracciones penales y por la que se deroga la Decisión 2000/642/JAI del Consejo (DO L 186 de 11.7.2019, p. 122).

24 Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión (DO L 141 de 5.6.2015, p. 73).

Las UIF también sirven de punto de contacto nacional para el intercambio transfronterizo de información. Al igual que los organismos de recuperación de activos, estas varían considerablemente entre Estados miembros en cuanto a su estructura organizativa, funciones y recursos. Dependen bien de autoridades judiciales, bien de cuerpos policiales, o son entidades híbridas que combinan competencias policiales y fiscalizadoras. Esta diversidad puede a veces crear obstáculos a la cooperación internacional.

No obstante, a la vista de la naturaleza transnacional del blanqueo de capitales y de la financiación del terrorismo, la coordinación y la cooperación entre las UIF revisten suma importancia. Para mejorar tal coordinación y cooperación y para garantizar que los informes sobre transacciones sospechosas lleguen a la UIF del Estado miembro en el que más útil sea el informe, se han fijado normas detalladas en la Directiva (UE) 2015/849. Con miras a proporcionar la más amplia cooperación transfronteriza de forma ágil, constructiva y eficaz, los Estados miembros deben asegurarse concretamente de que sus UIF intercambian información libremente, ya sea de manera espontánea o previa solicitud, con unidades de información financiera de terceros países.

Es importante mejorar el intercambio de información entre las UIF dentro de la Unión y utilizar instalaciones seguras, en particular, la red informática descentralizada FIU.NET. Las 28 UIF están conectadas a FIU.NET, que en los últimos años ha pasado de ser una herramienta básica segura para un intercambio bilateral estructurado de información a ser una herramienta multifuncional segura para el intercambio de información multilateral, con dispositivos de gestión de casos, así como procesos de normalización semiautomatizados. En FIU.NET, cada nuevo dispositivo o proceso automatizado es optativo, sin consecuencias derivadas. Las UIF individuales pueden decidir qué posibilidades y dispositivos ofrecidos por FIU.NET utilizan; solo utilizan los dispositivos con los que trabajan a gusto y excluyen los que no necesiten o no deseen utilizar.

1.11. Convenio de Nápoles II[25]

Los Estados miembros se asisten mutuamente en el marco del Convenio Nápoles II para prevenir y detectar infracciones a las disposiciones aduaneras nacionales y perseguir y castigar infracciones a las disposiciones aduaneras nacionales y comunitarias. En cuanto a las investigaciones penales, el Convenio establece procedimientos con arreglo a los cuales las administraciones aduaneras pueden actuar conjuntamente e intercambiar datos, espontáneamente o previa petición, relativos a actividades de tráfico ilícito.

Las solicitudes se presentan por escrito, en una lengua oficial del Estado miembro al que pertenezca la autoridad requerida, o bien en otra aceptada por esta. Mediante un formulario se establecen las normas para la transmisión de información. Las autoridades afectadas comunican toda la información que pueda ayudar a prevenir, detectar y perseguir infracciones. Intercambian datos personales, es decir, toda la información relativa a una persona física identificada o identificable.

En el marco de la asistencia que deba prestarse, la autoridad requerida, o la autoridad competente a la que haya recurrido esta última, procederá como si actuase por su propia cuenta o a instancia de otra autoridad de su propio Estado miembro.

El Prontuario para el Convenio de Nápoles II relativo a la asistencia mutua y la cooperación entre las administraciones aduaneras está dividido en tres partes, que contienen:

- las disposiciones generales, en 13615/05 ENFOCUSTOM 61 + COR 1 (CZ);
- las fichas nacionales, actualizadas en 2016, en 15429/16 JAI 1028 ENFOCUSTOM 238;
- los anexos, incluidos los formularios para la transmisión de información, en 13615/05 ENFOCUSTOM 61 ADD 1.

[25] Acto del Consejo, de 18 de diciembre de 1997, por el que se celebra, sobre la base del artículo K.3 del Tratado de la Unión Europea, el Convenio relativo a la asistencia mutua y la cooperación entre las administraciones aduaneras (DO C 24 de 23.1.1998, p. 1).

1.12. Unidad de Información sobre los Pasajeros

De conformidad con la Directiva 2016/681[26], cada Estado miembro publica o designa una unidad de información sobre los pasajeros (UIP). Dichas unidades son competentes para tratar datos procedentes del registro de nombres de los pasajeros o PNR recibidos de las compañías aéreas y[27], además, constituyen el principal canal de intercambio de información entre Estados miembros y con Europol. Dos o más Estados miembros podrán establecer o designar una autoridad única que actúe como su UIP.

El tratamiento de datos del PNR sirve principalmente para evaluar a los pasajeros con el fin de determinar aquellos que requieran un examen más detenido por parte de las autoridades nacionales competentes a efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves. La Directiva se aplica a los vuelos exteriores de la UE y puede aplicarse asimismo a los vuelos interiores de la UE en caso de que un Estado miembro así lo decida.

La evaluación de los datos PNR facilita la identificación de personas que, previamente a dicha evaluación, no eran sospechosas de estar implicadas en delitos de terrorismo o en delitos graves. En consonancia con la política de protección de datos de la UE, el tratamiento de dichos datos deberá ser a un tiempo pertinentes y necesario, así como proporcionado a los objetivos específicos de seguridad perseguidos por la Directiva.

---

26 Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (DO L 119 de 4.5.2016, p. 132).

27 La Directiva no afecta a la posibilidad de que los Estados miembros establezcan en su derecho nacional un mecanismo para recoger y tratar los datos PNR proporcionados por operadores económicos que no sean compañías aéreas, tales como agencias de viaje y operadores turísticos que prestan servicios relacionados con los viajes, como la reserva de vuelos, para los cuales recogen y tratan datos PNR, o de los transportistas que no sean los mencionados en él, siempre que el derecho nacional de que se trate respete el derecho de la Unión.

Las UIP son responsables:

- a escala nacional, de recopilar datos PNR de las compañías aéreas, almacenarlos y tratarlos y transmitir dichos datos o el resultado del tratamiento de los mismos, a las autoridades competentes;

- a escala de la Unión, intercambiar los datos PNR y el resultado de su tratamiento

    a) entre sí. No obstante, en casos de emergencia, y bajo determinadas condiciones, las autoridades nacionales competentes arriba indicadas podrán pedir a la UIP de otro Estado miembro que les proporcione directamente los datos PNR que se conserven en la base de datos de este último; y

    b) con Europol, que tendrá derecho, dentro de los límites de sus competencias y para el desempeño de sus funciones, a solicitar dichos datos de las UIP.

Las UIP desempeñarán sus funciones exclusivamente en un lugar seguro dentro del territorio de un Estado miembro. Los datos PNR facilitados a las UIP deberán conservarse en una base de datos por un período de cinco años tras su traslado a la UIP del Estado miembro de llegada o salida. No obstante, a los seis meses de su transferencia, todos los datos PNR deberán despersonalizarse, enmascarando aquellos elementos que figuran en la Directiva y que podrían servir para identificar directamente al interesado. Los resultados del tratamiento serán conservados por la UIP únicamente durante el tiempo necesario para informar de un resultado positivo a las autoridades nacionales competentes y a las UIP de otros Estados miembros.

La correspondiente UIP tratará únicamente aquellos datos que figuren en el Anexo I de la Directiva a los efectos de:

- realizar una evaluación de los pasajeros antes de su llegada o salida programada del Estado miembro, a fin de identificar a toda persona que deba ser examinada de nuevo por las autoridades competentes, y, en su caso, por Europol;

- responder en cada caso particular, a las peticiones de las autoridades competentes de que se suministren y traten datos PNR en casos específicos y facilitar a las autoridades competentes o, en su caso, a Europol, los resultados de dicho tratamiento;

- analizar los datos PNR con el fin de actualizar o establecer nuevos criterios a fin de identificar a toda persona que pueda estar implicada en un delito de terrorismo o delito grave.

Al realizar dichas evaluaciones, las UIP podrán, bien comparar los datos PNR con las bases de datos pertinentes con fines de prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y los delitos graves y, de acuerdo con las normas de la Unión, internacionales y nacionales aplicables a dichas bases de datos, bien tratar los datos PNR con arreglo a criterios predeterminados. Estos criterios previamente determinados deben ser orientados, proporcionados y específicos. Corresponde a las UIP establecer y revisar periódicamente tales criterios en cooperación con las autoridades competentes pertinentes. Tales criterios no deberán basarse en datos sensibles de carácter personal relacionados con la raza o el origen étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud o la vida u orientación sexual de la persona.

Respecto a las personas identificadas, la UIP de que se trate transmitirá todos los datos PNR pertinentes y necesarios o el resultado de su tratamiento a la correspondiente UIP del otro Estado miembro. Dichas UIP transmitirán la información recibida a sus propias autoridades competentes.

El responsable de la protección de datos nombrado por la UIP será el encargado de supervisar el tratamiento de los datos PNR. El interesado tendrá derecho a ponerse en contacto con el responsable de la protección de datos, como punto de contacto único, para todas las cuestiones relacionadas con el tratamiento de sus datos PNR.

Todas las transmisiones de datos PNR por las compañías aéreas a las UIP se efectuarán por medios electrónicos para garantizar la seguridad técnica. A tal efecto, se determinan a escala de la UE tanto los protocolos comunes a que deberán ajustarse las compañías aéreas al transmitir datos, como los formatos de datos admitidos que permiten la lectura de los datos por todas las partes pertinentes.[28]

[28] Decisión de Ejecución (UE) 2017/759 de la Comisión, de 28 de abril de 2017, relativa a los protocolos comunes y los formatos de datos que deberán utilizar las compañías aéreas para la transmisión de los datos PNR a las Unidades de Información sobre Pasajeros (DO L 113 de 29.4.2017, p. 48).

1.13. Puntos de acceso nacionales del SES

El Sistema de Entradas y Salidas[29] (SES) tiene como objetivo principal mejorar la gestión de las fronteras exteriores de la Unión, y a tal efecto lo utilizan las autoridades de fronteras, inmigración y visados[30]. El sistema registra electrónicamente el momento y el lugar de entrada y de salida de determinados nacionales de terceros países admitidos para una estancia de corta duración en el territorio de los Estados miembros, y calcula la duración de la estancia autorizada. El SES se utiliza en las fronteras exteriores. Los Estados miembros que aplican el acervo de Schengen íntegramente introducen el SES en sus fronteras interiores con los Estados miembros que no aplican aún el acervo de Schengen íntegramente, independientemente de que utilicen o no el SES. Los Estados miembros que no aplican plenamente el acervo de Schengen no introducen funcionalidades biométricas.

Además de las autoridades fronterizas, de inmigración y de visados, las «autoridades designadas» podrán consultar el SES con arreglo a las condiciones establecidas en el Reglamento. Realizan las consultas por motivos policiales, y para obtener información en las investigaciones relacionadas con delitos de terrorismo y otros delitos graves, en particular la identificación de los autores de tales delitos, de los sospechosos y de las víctimas, que hayan cruzado las fronteras exteriores.

Los Estados miembros designan a las autoridades habilitadas para consultar el SES con fines policiales. Además, cada Estado miembro designa un punto de acceso central al SES. Separado de las «autoridades designadas», el acceso central desempeña sus funciones con plena independencia de estas y no debe recibir instrucciones de ellas en cuanto al resultado de la verificación –es decir, el proceso de comparación de series de datos para determinar la validez de una identidad declarada–, con objeto de garantizar la independencia del proceso. Solo el personal debidamente habilitado del punto de acceso central está autorizado a acceder al SES.

---

29 Reglamento (UE) 2017/2226 del Parlamento Europeo y del 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 (DO L 327 de 9.12.2017, p. 20).

30 La Comisión determinará la fecha a partir de la cual deberá comenzar a funcionar el SES, una vez que se cumplan las condiciones establecidas en el artículo 66 del Reglamento (UE) 2017/2226.

Las unidades operativas de las «autoridades designadas» están autorizadas a solicitar los datos del SES a través de los puntos de acceso central. Para ello, la unidad operativa debe presentar a un punto de acceso central una solicitud electrónica o por escrito motivada para el acceso a los datos del SES. El punto de acceso central comprueba si se cumplen las condiciones de acceso establecidas en el Reglamento y, en caso de que así sea, trata la solicitud. Los datos del SES se transmitirán entonces a una unidad operativa de manera que no se comprometa la seguridad de los datos.

Las condiciones que deben comprobarse para acceder a los datos del SES con fines policiales son:

- el acceso para consulta es necesario a efectos policiales;
- el acceso para consulta es necesario y proporcionado en un caso concreto;
- existen pruebas o motivos fundados para considerar que la consulta de los datos del SES contribuirá a la prevención, detección o investigación de cualquiera de los delitos en cuestión, en particular cuando exista una sospecha fundada de que el sospechoso, el autor o la víctima de un delito de terrorismo o de otro delito grave están encuadrados en una categoría a la que es aplicable el Reglamento.

Además, se permitirá acceder al SES como herramienta para identificar al sospechoso, el autor o la víctima de dichos delitos cuando

- se haya realizado previamente una búsqueda en las bases de datos nacionales;
- en el caso de búsquedas con impresiones dactilares, se haya iniciado una búsqueda previa con arreglo a la Decisión del Consejo 2008/615/JAI («Decisión Prüm») cuando las comparaciones de impresiones dactilares sean técnicamente posibles, y tanto si dicha búsqueda se ha realizado íntegramente como si no se ha realizado íntegramente en un plazo de dos días desde su inicio.

Podrá presentarse una solicitud de consulta del VIS sobre el mismo titular de los datos, en paralelo a una solicitud de consulta del SES de conformidad con las condiciones establecidas en la Decisión 2008/633/JAI del Consejo[31].

Por último, se autorizará el acceso al SES como herramienta para consultar el historial de viaje o los períodos de estancia en el territorio de los Estados miembros de un sospechoso, autor o presunta víctima conocidos de un delito de terrorismo u otro delito grave, cuando se cumplan las condiciones arriba mencionadas.

1.14. Unidad nacional del SEIAV[32]

El Sistema Europeo de Información y Autorización de Viajes (SEIAV) es un soporte para[33] el intercambio de información a efectos de gestión de las fronteras, funciones policiales y lucha contra el terrorismo. Su objeto es determinar la admisibilidad de los nacionales de terceros países exentos de visado antes de que se desplacen al espacio Schengen y lleguen a los pasos fronterizos exteriores. El SEIAV establece una autorización de viaje que es, por naturaleza, independiente de un visado, pero constituye una condición de entrada y residencia e indica que el solicitante no supone una amenaza para la seguridad, un riesgo de inmigración ilegal ni un peligro elevado de epidemia.

El SEIAV está compuesto por

- el sistema de información del SEIAV, que incluye la lista de alerta rápida del SEIAV;
- la unidad central del SEIAV, que forma parte de la Agencia Europea de la Guardia de Fronteras y Costas;
- las unidades nacionales del SEIAV.

---

31 Decisión 2008/633/JAI del Consejo 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 crea 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). Reglamento (UE) 2018/1241 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se modifica el Reglamento (UE) 2016/794 con objeto de establecer el Sistema Europeo de Información y Autorización de Viajes (SEIAV), DO L 236 de 19.9.2018, p. 72.

33 La Comisión determinará la fecha a partir de la cual deberá comenzar a funcionar el SEIAV, una vez que se cumplan las condiciones establecidas en el artículo 88 del Reglamento (UE) 2018/1240.

Si en el procedimiento de solicitud automática se produce una coincidencia («respuesta positiva») entre los datos que figuran en el expediente de solicitud y los datos de los sistemas de información del SEIAV, los indicadores de riesgo específicos o las descripciones contenidas en los sistemas de información de la UE consultados, se encargará a la unidad central del SEIAV la tarea de verificar la respuesta positiva y, cuando se confirme la coincidencia o si persisten las dudas, de iniciar el tratamiento manual de la solicitud en el Estado miembro identificado.

Posteriormente, es la unidad nacional del SEIAV del Estado miembro de que se trate la que trata manualmente la solicitud en cuestión. Esta tendrá acceso al expediente de solicitud y a cualesquiera expedientes de solicitud vinculados, así como a cualquier respuesta positiva activada durante el tratamiento automatizado. Tras el tratamiento manual, la unidad nacional responsable podrá expedir o rechazar, de conformidad con las disposiciones del Reglamento, una autorización de viaje. Para ello, la unidad nacional puede solicitar información o documentación adicionales.

Una autorización de viaje debe denegarse si el solicitante:

- utiliza un documento de viaje que haya sido declarado perdido, robado o sustraído, o invalidado en el SIS;
- supone un riesgo para la seguridad;
- supone un riesgo de inmigración ilegal;
- supone un riesgo elevado de epidemia;
- es una persona para la cual se ha introducido en el SIS una descripción con el fin de que se le deniegue la entrada o la estancia;
- no responde a una petición de información o documentación adicionales o no acude a una entrevista;

Las unidades nacionales SEIAV se encargan del examen de las solicitudes y de la decisión de expedir o rechazar, anular o retirar las autorizaciones de viaje. Con este fin, han de cooperar entre ellas y con Europol para evaluar las solicitudes.

Una unidad nacional puede decidir denegar o anular una autorización de viaje cuando resulte evidente que las condiciones de expedición no se cumplían en el momento en que se expidió, o retirarla cuando resulte evidente que ya no se cumplen las condiciones para su expedición. Los solicitantes afectados tienen derecho a recurrir. Los recursos han de interponerse en el Estado miembro que haya adoptado la decisión de denegación, anulación o revocación de conformidad con el Derecho nacional de dicho Estado miembro. La unidad nacional competente se encarga de facilitar a los solicitantes información sobre el procedimiento de recurso.

Las autoridades fronterizas competentes para realizar inspecciones fronterizas en los pasos exteriores consultarán el sistema central del SEIAV utilizando los datos contenidos en la zona de lectura óptica del documento de viaje. Las autoridades de inmigración que comprueban o verifican si se cumplen las condiciones de entrada o estancia en el territorio de los Estados miembros tienen acceso para consultar el sistema central del SEIAV.

Solo en casos específicos, y solo cuando sea necesario para los fines de prevención, detección o investigación de delitos de terrorismo o de delitos graves, las autoridades policiales designadas por los Estados miembros tendrán derecho a solicitar la consulta de los datos personales registrados en el sistema central SEIAV. La Directiva (UE) 2016/680 («Directiva sobre la policía») se aplica al tratamiento de dichos datos personales por parte de las autoridades designadas de los Estados miembros con arreglo al Reglamento SEIAV.

1.15. Interoperabilidad

El principal objetivo del «paquete sobre interoperabilidad»[34] es mejorar la arquitectura de gestión de datos de la Unión para la gestión de las fronteras y la seguridad, con el fin de facilitar la correcta identificación de aquellas personas que no son ciudadanos europeos, sino nacionales de terceros países. La interoperabilidad entre el SES (véase el punto 3.18), el VIS (véase el punto 3.7), el SEIAV (véase el punto 3.19), Eurodac (véase el punto 3.8), el SIS (véase el punto 3.2) y el sistema ECRIS-TCN (véase el punto 3.13.2) tiene por objeto permitir que estos sistemas de información se complementen entre sí. Para ello, han de crearse 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)[35].

a) Para garantizar el uso sistemático de los sistemas de información de la UE mencionados, las autoridades designadas habilitadas para acceder al menos a uno de ellos, al RCDI y al DIM, a los datos de Europol o a las bases de datos de Interpol DVRP y TDAWN (véase el punto 2.4) deben utilizar el PEB, que permite consultar simultáneamente estos sistemas de información.

b) El registro común de datos de identidad (RCDI) crea un expediente individual para cada persona registrada en esos sistemas de información, y se entiende como un contenedor compartido para los datos de identidad, los datos de viaje y los datos biométricos de las personas registradas en los sistemas. EL RCDI debe ser parte de la arquitectura técnica de los sistemas y servir como componente compartido entre ellos para almacenar los datos de identidad, los datos del viaje y los datos biométricos que procesan.

---

[34] 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 de 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 modifica los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).

[35] La Comisión determinará la fecha a partir de la cual deberán comenzar a aplicarse las disposiciones de los Reglamentos relacionadas con el PEB, el SCB compartido, el RCDI y el DIM.

El acceso al RCDI se concede para fines como

- la identificación correcta de la persona registrada en los sistemas de información de la UE o, en caso necesario,

- asistir a las autoridades policiales en la prevención, detección e investigación de delitos de terrorismo o de delitos graves;

Cuando por distintas razones una autoridad policial no consiga identificar a una persona, puede consultar el RCDI. Con este fin, los Estados miembros facultarán a su autoridad competente, con arreglo a la legislación nacional, para realizar la consulta y establecerán los procedimientos, condiciones y criterios para realizar las comprobaciones. La consulta se lleva a cabo a partir de las impresiones dactilares recién tomadas de dicha persona, o bien, si no existe esa posibilidad, a partir de los datos de identidad de la persona combinados con los datos del documento de viaje.

En caso de que la consulta indique que los datos sobre esa persona están almacenados en el RCDI, la autoridad policial obtendrá los apellidos, nombre, fecha de nacimiento, lugar de nacimiento, nacionalidad, género, nombres anteriores si procede, pseudónimos o alias cuando se disponga de ellos, así como, cuando sea pertinente, información sobre documentos de viaje. Además, si así lo contempla la legislación nacional, la policía podrá realizar consultas sobre datos biométricos en caso de catástrofe natural, accidente o ataque terrorista, y únicamente a efectos de identificación de personas desconocidas que no puedan identificarse por sí mismas o de restos humanos no identificados.

Al consultar el RCDI con fines policiales, en particular cuando se sospeche que el sospechoso, el autor o la víctima de un delito de terrorismo o de un delito grave son personas cuyos datos están almacenados en los sistemas de información, las autoridades designadas y Europol podrán consultar el RCDI para saber si se almacenan datos sobre una persona concreta. En caso afirmativo, tras la verificación automática de la existencia de una coincidencia en el sistema (marcador de respuesta positiva y negativa), el RCDI facilita una respuesta en forma de referencia que indica cuál es el sistema de información que contiene datos coincidentes. La respuesta en forma de aviso de correspondencia debe utilizarse únicamente a efectos de presentar una solicitud de acceso al sistema de información de la UE reseñado. Dicha respuesta no debe revelar datos personales de la persona de que se trate, aparte de la indicación de que 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. Se considera, por lo tanto, que el acceso del usuario final a un aviso de correspondencia supone 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 solicitar el acceso a datos personales de forma más eficaz. El acceso total a los datos con fines policiales sigue estando sujeto a las condiciones y procedimientos establecidos en el Reglamento Eurodac (véase el punto 2.7).

c) El detector de identidades múltiples (DIM) crea y almacena los vínculos entre los datos de los distintos sistemas de información de la UE. En el ámbito policial: el DIM del RCDI y del SIS se pondrá en marcha cuando se cree o actualice una descripción de una persona en el SIS, o cuando se cree o modifique un registro de datos en el ECRIS-TCN. Únicamente se iniciará con el fin de comparar los datos disponibles en un sistema de información de la UE con los datos disponibles en otro sistema de información de la UE. La verificación de las distintas identidades la realizarán manualmente el Servicio Nacional Sirene o las autoridades centrales respectivas.

La Comisión:

- determinará la fecha a partir de la cual deberán comenzar a aplicarse las disposiciones de los Reglamentos relacionadas con el PEB, el SCB compartido, el RCDI y el DIM;

- en estrecha cooperación con los Estados miembros, la 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.

1.16. Elección del cauce - Criterios utilizados habitualmente

En un Estado miembro, el PUC[36] desempeña una función crucial en la determinación del cauce mas apropiado y pertinente para recibir todas las solicitudes (tanto entrantes como salientes) tratadas por la unidad. Por razones de eficacia, las autoridades nacionales conceden una gran autonomía a los investigadores para que elijan la vía que consideran más adecuada a la investigación. Los canales de comunicación más habitualmente utilizados son los siguientes:

[36] Directrices sobre un punto único de contacto (SPOC), 10492/14 DAPIX 75 ENFOPOL 157 y 10492/14 DAPIX 75 ENFOPOL 157 ADD 1 REV 1).

- Sirene a través de los puntos de contacto de cada Estado Schengen para el SIS
- EUROPOL a través de las unidades nacionales de Europol / los funcionarios de enlace de Europol
- Interpol, a través de las Oficinas Centrales Nacionales en las Direcciones Generales de la Policía
- Funcionarios de enlace
- Canales de asistencia mutua utilizados entre autoridades aduaneras (Nápoles II)
- Canales bilaterales basados en acuerdos de cooperación a escala nacional, regional y local (CCPA)

Las normas generales establecen que una solicitud se remite por un único canal. Sin embargo, en casos excepcionales, una solicitud puede remitirse por diferentes canales al mismo tiempo. En tales casos, este extremo se indicará claramente a todas las partes de un modo adecuado. Del mismo modo, un cambio de canal debe comunicarse a todas las partes, junto con los motivos del cambio.

Para evitar solapamientos temáticos o situaciones en las que una solicitud se remite innecesariamente mas de una vez a través de distintos canales, el encargado respectivo (SIS, Europol, Interpol, funcionario de enlace bilateral) en el Estado requirente podrá determinar el conducto mas adecuado para una solicitud de información sobre la base de los siguientes criterios:

- criterios geográficos, a saber se conoce la nacionalidad, residencia u origen de la persona u objeto de que se trate y la solicitud se refiere a la comunicación de datos concretos (dirección postal, número de teléfono, impresiones dactilares, ADN, registro, etc.)
- criterios temáticos, a saber: delincuencia organizada, delito grave, terrorismo; confidencialidad/sensibilidad; canal utilizado para una solicitud anterior relacionada
- criterios técnicos, a saber: la necesidad de unos canales de información seguros
- criterios de urgencia, a saber: un riesgo inmediato para la integridad física de una persona, perdida inmediata de una prueba, solicitud de operaciones o vigilancia transfronteriza urgente

2. SISTEMAS DE INFORMACIÓN

2.1. El Sistema de Información de Schengen – segunda generación (SIS II)[37]

El Sistema de Información de Schengen de segunda generación («SIS II») está actualmente en funcionamiento en 26 Estados miembros de la UE, así como en cuatro países de fuera de la UE asociados a la cooperación de Schengen: Noruega, Islandia, Suiza y Liechtenstein. Apoya la cooperación operativa entre autoridades policiales y autoridades judiciales en asuntos penales. Puesto que el SIS es tanto una cooperación policial como un sistema de control aduanero, una selección de funcionarios policiales, guardias de fronteras, funcionarios de aduanas y autoridades judiciales y de visados en todo el espacio Schengen pueden consultar el SIS.[38]

Los datos del SIS II pueden buscarse (sujeto a normas estrictas en materia de protección de datos) las 24 horas del día y los 7 días de la semana a través de las Oficinas SIRENE, en los puntos de control fronterizo y en los consulados en el exterior. La base de datos conserva datos sobre **personas** y **objetos**, y permite el intercambio de datos con objeto de prevenir delitos y luchar contra la inmigración irregular. Mediante una búsqueda en línea en el SIS, el funcionario que consulta establece rápidamente, en función de si hay o no respuesta positiva, si una persona buscada figura en la base de datos o no.

Los datos se refieren a descripciones (una descripción es una serie de datos que permiten a las autoridades identificar personas u objetos con vistas a tomar las medidas oportunas):

Descripciones de **personas**, relativas a ciudadanos de la UE y de fuera de la UE. Facilitan medidas tales como:

- detención a efectos de entrega basada bien en la Orden de detención europea o en acuerdos celebrados entre la UE y terceros países o a efectos de extradición;
- búsqueda del paradero de personas desaparecidas;
- citaciones para comparecer ante un órgano judicial en el contexto de un procedimiento penal o de la ejecución de una sentencia que conlleve privación de libertad;

---

37 Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), DO L 205 de 7.8.2007, p. 63.

38 Una lista de lista de las autoridades nacionales competentes que tienen derecho a acceder a las descripciones se publica anualmente en el *Diario Oficial de la Unión Europea*.

– vigilancia discreta y controles específicos con objeto de perseguir delitos penales, prevención de amenazas a la seguridad pública o prevención de amenazas a la seguridad nacional;

– denegación de entrada en el territorio Schengen a nacionales o extranjeros como resultado de una decisión administrativa o judicial, o por motivos de amenaza para el orden público o la seguridad nacional, o por motivos de incumplimiento de obligaciones nacionales de entrada y residencia de extranjeros.

Se introducen descripciones de **objetos** en el SIS II a efectos de vigilancia discreta o controles específicos, incautación, prueba en procesos penales o vigilancia. Dichas descripciones se refieren a:

– vehículos, barcos, aeronaves, contenedores

– armas de fuego

– documentos robados

– billetes de banco

– propiedades robadas tales como objetos de arte, botes, buques.

Personal de Europol específicamente autorizado tiene derecho, en el ámbito de su mandato, a acceder y buscar directamente datos introducidos en el SIS II y puede pedir más información al Estado miembro de que se trate.

Los miembros nacionales de Eurojust y sus asistentes tienen derecho, en el ámbito de su mandato, a acceder y buscar datos introducidos en el SIS II.

2.2. SIE – Sistema de información de Europol[39]

El Reglamento Europol introduce un nuevo concepto para el tratamiento de datos, que suele denominarse modelo integrado de gestión de datos. El modelo integrado de gestión de datos puede definirse como la posibilidad de utilizar información relacionada con la comisión de delitos para múltiples objetivos operativos conforme a las indicaciones del propietario de los datos, lo que posibilita su gestión y tratamiento de forma integrada y tecnológicamente neutra. Con arreglo a la Decisión del Consejo sobre Europol, el tratamiento de datos se estructuraba en torno a sistemas. El Reglamento Europol ya no hace referencia a los sistemas; en su lugar, estipula que debe indicarse la finalidad del tratamiento de datos. Para facilitar una transición gradual, los usuarios pueden seguir trabajando con los sistemas existentes de un modo que sea compatible con el nuevo marco jurídico.

El sistema de información de Europol (SIE), al que hace referencia la Decisión sobre Europol, es un sistema centralizado alojado en Europol que permite a los Estados miembros y a los socios de la cooperación de Europol almacenar, compartir y cruzar datos relacionados con sospechosos, condenados o «futuros delincuentes potenciales» implicados en delitos que correspondan al mandato de Europol (delitos graves, delincuencia organizada o terrorismo). Permite almacenar toda la gama de datos y pruebas relacionados con estos delitos y personas, por ejemplo personas con alias, empresas, números de teléfono, direcciones de correo electrónico, vehículos, armas de fuego, ADN, fotos, impresiones dactilares, bombas, etc. El SIE, que sirve en primer lugar de sistema de apoyo a las comprobaciones cruzadas, proporciona un acceso basado en un sistema de respuesta positiva o negativa. El Reglamento Europol prevé un acceso pleno a los datos remitidos para el análisis temático o estratégico, pero solo un acceso basado en un sistema de respuesta positiva o negativa por lo que respecta a los datos proporcionados para el análisis operativo.

El SIE es de hecho un sistema de referencia que ayuda a determinar si la información buscada está disponible o no en uno de los Estados miembros, en los socios de la cooperación o en Europol. Está directamente disponible en todos los Estados miembros y para el personal debidamente autorizado de Europol. Actualmente, los Estados miembros pueden introducir datos de tres formas diferentes:

a) inserción manual de datos en el SIE o a través de la aplicación SIENA;

[39] 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, aplicable desde el 1 de mayo de 2017).

b) transferencia semiautomatizada de datos mediante una carga por lotes en el SIE;

c) transferencia automatizada de datos mediante un cargador de datos.

La gran mayoría de datos se introducen en el sistema de información de Europol (SIE) mediante sistemas de carga de datos automatizados. El planteamiento de los Estados miembros en materia de recopilación de datos ha cambiado, al centrarse en transmitir a las entidades un cambio de datos que puedan cruzarse, tales como personas, vehículos, números de teléfono y armas de fuego.

Los países terceros no pueden introducir directamente ni cruzar datos en el SIE, pero sí pueden remitirlos a Europol, de conformidad con el artículo 23, apartado 5, del Reglamento Europol. Europol tendrá que evaluar en primer lugar si los datos están dentro de su mandato y solo entonces los aceptará y realizará las comprobaciones cruzadas.

El SIE, que permite compartir información muy sensible, dispone de un robusto sistema que garantiza la confidencialidad y la seguridad. La seguridad está garantizada, por ejemplo, con los códigos de tratamiento específicos. Indican lo que se puede hacer con una determinada información y quien tiene acceso a ella. Los códigos de tratamiento están concebidos para proteger la fuente de información y garantizar que el tratamiento de la información es conforme con los deseos del propietario de la información y con la legislación nacional de los Estados miembros. El SIE está acreditado para el tratamiento de datos hasta la categoría EU RESTRICTED incluida.

2.3. SIENA - Aplicación de la Red de Intercambio Seguro de Información de Europol

SIENA es el sistema de comunicación seguro de Europol utilizado por los Estados miembros y sus socios de cooperación para intercambiar datos e información estratégicos y operativos relacionados con delitos, incluidos datos operativos sobre personas. SIENA es un sistema de mensajería que ofrece diferentes tipos de mensajes para diferentes fines, incluido el intercambio de datos con arreglo a la «Decisión Marco sueca».

En la concepción y funcionamiento de SIENA se insistió en la seguridad, la protección de datos y la confidencialidad. SIENA está acreditado para el intercambio de información clasificada como EU CONFIDENTIAL. El intercambio de datos a través de SIENA supone responsabilidades claras en materia de tratamiento de datos. Para cada mensaje SIENA enviado fuera, es preciso indicar la clasificación (confidencialidad), los códigos de tratamiento y la fiabilidad de la fuente y la información.

La lengua predeterminada del interfaz de usuario SIENA es el inglés, mientras que el interfaz es multilingüe, lo que permite a los operadores SIENA trabajar en su(s) propia(s) lengua(s) nacional(es). Además de intercambiar mensajes, los operadores SIENA pueden realizar búsquedas y crear informes estadísticos sobre los datos intercambiados a través de SIENA.

SIENA es un soporte para el intercambio de datos bilateral entre Estados miembros y permite a los Estados miembros intercambiar datos fuera del mandato de Europol. Cuando el intercambio de datos se dirija a uno de los socios de la cooperación Europol, se notificará a los Estados miembros a través de SIENA de que este intercambio solo debe realizarse si se refiere a delitos que son competencia de Europol.

Europol solo tratará la información intercambiada a través de SIENA a efectos de tratamiento de datos operativos si se incluyó a Europol como destinatario en el intercambio de datos. A efectos de auditoría, todos los datos intercambiados a través de SIENA están a disposición del responsable de la protección de datos de Europol y las autoridades nacionales de control.

SIENA es un soporte para el intercambio de datos estructurado basado en el Formato de mensaje universal (UMF). En la actualidad, la entidad UMF PERSONA puede crearse/mostrarse en la propia aplicación web de SIENA. El servicio de web SIENA ya soporta el modelo completo de datos de UMF.

2.4. I-24/7 - Sistema mundial de comunicación policial de Interpol

La red mundial I-24/7 para el intercambio de información policial conecta la Secretaría General de Interpol en Lyon, Francia, las Oficinas Centrales Nacionales (OCN) y las oficinas regionales.

El Sistema de información de Interpol permite comunicar mensajes directamente entre OCN. Todas las bases de datos Interpol (salvo la bases de datos sobre imágenes de explotación sexual infantil) son accesibles en tiempo real a través del sistema de comunicación policial mundial I-24/7. El sistema I-24/7 también permite a los Estados miembros acceder mutuamente a sus bases de datos nacionales utilizando una conexión empresa a empresa (B2B). Los países miembros gestionan y llevan sus propios datos penales nacionales y controlan su presentación, acceso por otros países y la destrucción de datos de conformidad con su legislación nacional. Asimismo disponen de la opción de hacerlo accesible a la comunidad que aplica el Derecho Internacional a través de I-24/7.

2.4.1. Interpol: pasarela ADN

La base de datos ADN de Europol incluye una base de datos ADN internacional, un formulario de solicitud de búsqueda internacional para intercambio bilateral y una función para la transferencia electrónica normalizada segura. No se conservan datos nominales que relacionen un perfil de ADN con una persona. La pasarela ADN es compatible con el intercambio automatizado de datos de Prüm.

Los países miembros pueden acceder a la base de datos y, previa petición, el acceso puede ampliarse más allá de las Oficinas Centrales Nacionales a centros forenses y laboratorios. En los países miembros, la Policía puede presentar un perfil de ADN de delincuentes, lugares del crimen, personas desaparecidas y cuerpos sin identificar.

2.4.2. Base de datos de huellas dactilares de Interpol

Los usuarios autorizados en los países miembros pueden ver, presentar y cruzar registros a través de un sistema automático de identificación dactilar (SAID). Los registros se guardan e intercambian en el formato definido por el Instituto nacional de normas y tecnologías (NIST). Las Directrices relativas a transmisión de huellas dactilares y las Directrices relativas a transmisión de marcas de huellas dactilares en el lugar del crimen ayudan a los países miembros a mejorar la calidad y cantidad de registros de huellas dactilares introducidos en el SAID de Interpol.

2.4.3. Base de datos de documentos de viaje perdidos o robados de Interpol

La base de datos de documentos de viaje perdidos o robados de Interpol conserva información sobre más de 45 millones de documentos de viaje extraviados o robados introducidos por 166 países. Esta base de datos permite a la OCN de Interpol y a otros servicios policiales autorizados (como funcionarios de servicios de inmigración y control fronterizo) determinar la validez de un documento de viaje sospechoso. A efectos de prevenir y combatir delitos graves y organizados, los cuerpos y fuerzas de seguridad de los Estados miembros intercambian datos sobre pasaportes con Interpol.[40]

2.4.4. Documentos de viaje asociados a notificaciones (TDAWN)

La base de datos TDAWN contiene información sobre los documentos de viaje vinculados a personas que son objeto de una notificación de Interpol.

2.4.5. Cuadro de Referencia sobre Armas de Fuego

El Cuadro de Referencia de Interpol sobre Armas de Fuego permite a los investigadores identificar correctamente un arma de fuego utilizada en un delito (su fabricación, modelo, calibre, etc.). Contiene mas de 250.000 referencias de armas de fuego y 57.000 imágenes de alta calidad. La Red de Interpol de Información sobre Balística es una plataforma internacional para difundir y comparar datos balísticos a gran escala, y posee mas de 150.000 registros.

El Sistema de Interpol para la Gestión de los Registros y el Rastreo de Armas Ilícitas (iARMS) es una aplicación con tecnología informática que facilita un intercambio de información y una cooperación entre cuerpos y fuerzas de seguridad sobre armas de fuego relacionadas con delitos.

[40] Posición Común 2005/69/JAI del Consejo relativa al intercambio de determinados datos con Interpol (DO L 27 de 29.1.2005, p. 61).

2.5. Sistema Europeo de Información de Antecedentes Penales (ECRIS)[41]

El Sistema Europeo de Información de Antecedentes Penales (ECRIS)[42] basado en soluciones informáticas ofrece los medios electrónicos para intercambiar información sobre condenas entre Estados miembros en un formato normalizado. El ECRIS se utiliza para informar a los Estados miembros sobre condenas de sus nacionales y para enviar solicitudes de información sobre condenas a efectos de procesos penales y otros fines, tales como administrativos o laborales. Asimismo resulta posible enviar solicitudes sobre nacionales de países terceros si existe un motivo para creer que el Estado miembro requerido conserva información sobre esta persona.

Es preciso contestar a las solicitudes ECRIS en un plazo de diez días hábiles cuando la solicitud sea para un procedimiento penal o con fines laborales, y en plazo de veinte días hábiles si la solicitud fue cursada por una persona para su propia información.

ECRIS no está concebido para crear ninguna base de datos de registros penales centralizada y está basado en una configuración informática descentralizada en la que todos los registros penales se almacenan solamente en bases de datos gestionadas por Estados miembros. Los datos se intercambian electrónicamente entre las autoridades centrales de los Estados miembros designadas.

Los Estados miembros deberán transmitir la información de acuerdo con las normas y los formatos normalizados acordados, y esta deberá ser lo más completa posible para que el Estado miembro receptor pueda procesar la información adecuadamente e identificar a la persona. Los mensajes se envían en las lenguas oficiales de los Estados miembros afectados o en otra aceptada por ambos Estados miembros.

---

41 Decisión Marco 2009/315/JAI del Consejo, de 26 de febrero de 2009, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros (DO L 93 de 7.4.2009, p. 23).

42 Directiva (UE) 2019/884 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por la que se modifica la Decisión Marco 2009/315/JAI del Consejo en lo que respecta al intercambio de información sobre nacionales de terceros países y al Sistema Europeo de Información de Antecedentes Penales (ECRIS) y por la que se sustituye la Decisión 2009/316/JAI del Consejo (DO L 171 de 7.6.2019, p. 143 y DO L 151 de 7.6.2019, p. 143).

La Secretaría General del Consejo publicó un manual no vinculante para profesionales que presenta los procedimientos de intercambio de información y coordina su actuación para el desarrollo y funcionamiento del ECRIS y está disponible en formato electrónico en la página web del Consejo y en el sitio web CIRCABC albergado por la Comisión Europea en https://circabc.europa.eu/faces/jsp/extension/wai/navigation/container.jsp. Las solicitudes de acceso al manual deben remitirse a la Secretaría del Consejo. Las solicitudes de acceso al Grupo de interés restringido «Apoyo técnico y empresarial ECRIS» deben remitirse a la Comisión Europea.

2.5.1. El ECRIS-TCN[43]

El marco legal del ECRIS no aborda suficientemente las particularidades y solicitudes relativas a nacionales de terceros países. Dentro de la Unión, la información sobre nacionales de terceros países no se recoge como se hace con la de los nacionales de los Estados miembros, sino que únicamente se conserva en los Estados miembros en que se hayan impuesto las condenas. Por medio del ECRIS-TCN[44], la autoridad nacional central puede averiguar qué otros Estados miembros poseen información sobre antecedentes penales de un nacional de un tercer país. Después puede utilizarse el marco del ECRIS para solicitar dicha información a los Estados miembros en cuestión, de conformidad con la Decisión Marco 2009/315/JAI.

El Reglamento contiene disposiciones por las que se establece un sistema centralizado a escala de la Unión que contiene datos personales, así como disposiciones sobre el reparto de responsabilidades entre el Estado miembro y la organización responsable del desarrollo y mantenimiento del sistema centralizado. Establece un grado general adecuado de protección de los datos, seguridad de los datos y protección de los derechos fundamentales de las personas afectadas.

---

43 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 (NTP) a fin de complementar y apoyar el Sistema Europeo de Información de Antecedentes Penales (ECRIS-TCN) y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 1).
Directiva (UE) 2019/884 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por la que se modifica la Decisión Marco 2009/315/JAI del Consejo en lo que respecta al intercambio de información sobre nacionales de terceros países y al Sistema Europeo de Información de Antecedentes Penales (ECRIS) y por la que se sustituye la Decisión 2009/316/JAI del Consejo (DO L 171 de 7.6.2019, p. 143).

44 La Comisión determinará la fecha a partir de la cual deberá comenzar a funcionar el ECRIS-TCN, una vez que se cumplan las condiciones establecidas en el artículo 35 del Reglamento (UE) 2019/816.

Los Estados miembros deben crear en el ECRIS-TCN registros relativos a los nacionales de terceros países condenados. Esto debe hacerse, siempre que sea posible, de forma automática, y sin demoras indebidas a partir del momento en que la condena haya sido inscrita en el registro nacional de antecedentes penales. Los Estados miembros, de conformidad con lo dispuesto en dicho Reglamento, deben consignar en el sistema central los datos alfanuméricos y dactiloscópicos relativos a condenas pronunciadas después de la fecha en que se comiencen a introducir datos en el ECRIS-TCN. A partir de esa misma fecha, o en cualquier momento posterior, los Estados miembros deben poder introducir imágenes faciales en el sistema central.

El ECRIS-TCN permite el tratamiento de datos dactiloscópicos con el fin de identificar los Estados miembros poseedores de información sobre los antecedentes penales de un nacional de un tercer país. También debe permitir el tratamiento de imágenes faciales para confirmar su identidad. Es esencial que la introducción y utilización de los datos dactiloscópicos e imágenes faciales no excedan de lo estrictamente necesario para alcanzar el fin perseguido, respeten los derechos fundamentales, al igual que el interés superior de los menores, y sean conformes con las normas de la Unión aplicables en materia de protección de datos.

Eurojust, Europol y la Fiscalía Europea, deben tener acceso al ECRIS-TCN para identificar a los Estados miembros que posean información sobre antecedentes penales de un nacional de un tercer país, con el fin de poder desempeñar las funciones que le han sido encomendadas.

La Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (la «eu-Lisa» se encarga de desarrollar y gestionar el ECRIS-TCN.

2.6. Sistema de Información de Visados (VIS)[45]

El Sistema de Información de Visados (VIS) es principalmente un sistema de control de la inmigración. Se trata de una herramienta utilizada para facilitar la consulta a nivel de consulados y controles fronterizos mediante la verificación electrónica y el intercambio de datos sobre visados entre Estados miembros. Como tal, se centra en los nacionales extranjeros con obligación de visado. Se permite a las autoridades designadas por los Estados miembros (es decir, representaciones consulares, puntos de control fronterizo, autoridades policiales y de inmigración[46]) y Europol[47], en el marco de sus funciones, consultar el VIS[48] con fines de prevención, detección e investigación de:

- «delitos de terrorismo» son los delitos tipificados en la legislación nacional que corresponden o son equivalentes a los delitos contemplados en los artículos 1 a 4 de la Decisión Marco 2002/475/JAI del Consejo, de 13 de junio, sobre la lucha contra el terrorismo, y

- «delitos graves» son las formas de delincuencia que corresponden o son equivalentes a aquellas a que se refiere el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI («Orden de detención europea»).

---

45 Decisión del Consejo de 8 de junio de 2004 por la que se establece el Sistema de Información de Visados (VIS) (2004/512/CE) (DO L 213 de 15.6.2004, p. 5).

46 Lista de las autoridades competentes cuyo personal debidamente autorizado tendrá acceso al sistema para introducir, modificar, suprimir o consultar datos en el Sistema de Información de Visados (VIS) (2016/C 187/04) (DO C 187 de 26.5.2016, p. 4).

47 Decisión 2008/633/JAI del Consejo 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); Decisión 2013/392/UE del Consejo por la que se establece la fecha a partir de la cual surtirá efecto la Decisión 2008/633/JAI 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 198 de 23.7.2013, p. 45).

48 El 16 de abril de 2015, el Tribunal de Justicia Europeo anuló la Decisión 2013/392/UE del Consejo, de 22 de julio de 2013, por la que se establece la fecha a partir de la cual surtirá efecto la Decisión 2008/633/JAI 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. Con todo, el Tribunal declaró que los efectos de la Decisión 2013/392 debían mantenerse hasta la entrada en vigor de un nuevo acto que la sustituya.

De acuerdo con la Decisión Marco sueca, las autoridades competentes de los Estados miembros cuyas autoridades designadas tienen acceso al VIS pueden facilitar al Reino Unido y a Irlanda la información incluida en el VIS, y la información conservada en los registros de visados nacionales del Reino Unido e Irlanda puede transmitirse a las autoridades competentes de los cuerpos y fuerzas de servicios de seguridad de los otros Estados miembros.

El VIS está basado en una configuración centralizada y una plataforma común con el SIS II. Los datos del VIS se procesan en dos fases. En la primera, los datos incluyen datos alfanuméricos y fotografías. En la segunda, los datos biométricos y los documentos escaneados se procesan e introducen en el VIS. El VIS incluye datos sobre las solicitudes de visados, fotografías, impresiones dactilares, decisiones relacionadas de las autoridades responsables de los visados y enlaces entre aplicaciones relacionadas. El VIS utiliza un sistema de correspondencia biométrica para garantizar comparaciones de impresiones dactilares fiables a efectos de:

- verificación: controlar si unas impresiones dactilares escaneadas en el punto de cruce fronterizo corresponden a las asociadas con el registro biométrico adjunto al visado; o

- identificación: comparar las impresiones dactilares tomadas en el punto de cruce fronterizo con el contenido de toda la base de datos.

Técnicamente hablando, el VIS está compuesto por tres niveles, a saber: el central, el nacional y el local; este último incluye representaciones consulares, puntos de cruce fronterizo y autoridades policiales y de inmigración.
En mayo de 2018, la Comisión presentó una propuesta legislativa por la que se modificaba el Reglamento VIS, con el fin, entre otras cosas, de garantizar la interoperabilidad entre otras bases de datos en el ámbito de la Justicia y los Asuntos de Interior. No se espera que el VIS mejorado sea operativo antes de finales de 2021.

2.7. Eurodac[49][50]

Eurodac en primer lugar ayuda a determinar el Estado miembro responsable del examen de las solicitudes de asilo presentadas en uno de los Estados miembros y también facilita la aplicación del Convenio de Dublín. El acceso a Eurodac a efectos de prevenir, detectar o investigar delitos terroristas u otros delitos penales graves se da únicamente en casos bien definidos.

El Reglamento Eurodac 603/2013 establece disposiciones sobre la transmisión de datos dactiloscópicos a la Unidad Central, el registro de dichos datos y de otros datos pertinentes en la base de datos central pertinente, la conservación de los datos, la comparación con otros datos dactiloscópicos, la transmisión de los resultados de dicha comparación y el bloqueo y supresión de los datos registrados.

La configuración del sistema Eurodac comprende a) una base de datos central informatizada sobre impresiones dactilares («sistema central») compuesto por una unidad central y un plan y un sistema de continuidad de las actividades, y b) una infraestructura de comunicación entre el sistema central y los Estados miembros que ofrece una red virtual encriptada dedicada a datos Eurodac («infraestructura de comunicación»).

Cada Estado miembro dispone de un único Punto de Acceso Nacional.

La eu-LISA, creada en virtud del Reglamento (UE) 1077/2011[51], se encarga de la gestión operativa de Eurodac, y garantizará, en colaboración con los Estados miembros, que en todo momento se utilicen en el sistema central las mejores y más seguras técnicas y tecnologías disponibles, sujetas a un análisis de costes y beneficios.

---

49 Reglamento (CE) n.º 2725/2000 del Consejo, de 11 de diciembre de 2000, relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín (DO L 316 de 15.12.2000, p. 1).

50 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.º 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 (refundición).

51 Reglamento (UE) n.º 1077/2011 del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, por el que se establece una Agencia Europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia (DO L 286 de 1.11.2011, p. 1).

Cualquier Estado miembro puede transmitir impresiones dactilares a la unidad central para comprobar si un extranjero de al menos 14 años encontrado legalmente en su territorio ya ha presentado una solicitud de asilo en otro Estado miembro. La unidad central compara dichas impresiones dactilares con datos de impresiones dactilares transmitidos por otros Estados miembros y ya almacenados en la base de datos central. La unidad informa al Estado miembro que transmitió los datos si hay una respuesta positiva, es decir, el resultado de la comparación entre las impresiones dactilares registradas y las enviadas. El Estado miembro comprueba el resultado y procede a la identificación final en cooperación con los Estados miembros interesados.

Los Estados miembros velarán por la legalidad, precisión y seguridad de los datos Eurodac. Cualquier persona o Estado miembro que haya sufrido un daño como consecuencia de un incumplimiento de las disposiciones Eurodac tiene derecho a una compensación del Estado miembro responsable del daño sufrido.

El Reglamento (UE) n.º 603/2013 establece el acceso a las datos de Eurodac por parte de las autoridades designadas por los Estados miembros y por Europol a efectos policiales y judiciales. Con arreglo al Reglamento, las autoridades designadas pueden remitir una solicitud electrónica motivada de comparación de los datos de impresiones dactilares con los datos almacenados en el sistema central únicamente si las comparaciones con las siguientes bases de datos no permitieron determinar la identidad de la persona:

– Bases de datos dactiloscópicos nacionales.

– Los sistemas automatizados de identificación dactilar (SAID) de todos los demás Estados miembros en virtud de la Decisión 2008/615/JAI del Consejo («Decisiones Prüm») cuando la comparación sea posible desde el punto de vista técnico, a menos que existan motivos fundados para creer que la comparación con estos sistemas no va a permitir establecer la identidad del sujeto de los datos. Estos motivos razonables se incluirán en la solicitud electrónica motivada de comparación con datos Eurodac remitida por la autoridad designada a la autoridad verificadora.

– El Sistema de Información de Visados (VIS) siempre que se cumplan las condiciones para tal comparación previstas en la Decisión 2008/633/JAI.

Es preciso cumplir también las siguientes condiciones acumulativas:

a) Que la comparación sea necesaria a efectos de prevención, detección o investigación de delitos de terrorismo o de otros delitos graves, es decir, que exista un interés superior de seguridad pública que haga que la consulta de la base de datos sea proporcionada.

b) Que la comparación sea necesaria en un caso concreto (es decir, no se llevarán a cabo comparaciones sistemáticas).

c) Que existan motivos razonables para considerar que la comparación contribuirá sustancialmente a la prevención, detección o investigación de cualquiera de los delitos en cuestión. Existirán estos motivos razonables, en particular, cuando haya una sospecha fundada de que el sospechoso, el autor o la víctima de un delito de terrorismo o de otro delito grave están encuadrados en una categoría contemplada en el Reglamento n.º 603/2013.

2.8. SIA – Sistema de Información Aduanero[52]

El Sistema de Información Aduanero complementa el Convenio de Nápoles II[53]. El sistema pretende mejorar la administración aduanera de los Estados miembros mediante un intercambio rápido de información para prevenir, investigar y perseguir violaciones graves de legislación comunitaria y nacional. El SIA también crea un fichero de identificación de los expedientes de investigaciones aduaneras (FIDE) para ayudar en las investigaciones aduaneras.

El SIA, gestionado por la Comisión, es un sistema de información centralizado accesible a través de terminales en cada Estado miembro y en la Comisión, Europol y Eurojust. Las autoridades nacionales en materia de aduanas, fiscalidad, agricultura, sanidad pública y policía, Europol y Eurojust pueden acceder a los datos del SIA. Únicamente las autoridades designadas por los Estados miembros[54] y la Comisión disponen de acceso directo a los datos contenidos en el SIA. Para mejorar la complementariedad, Europol y Eurojust disponen de un acceso «solo lectura» al SIA y FIDE.

---

52 Decisión 2009/917/JAI del Consejo, de 30 de noviembre de 2009, sobre la utilización de la tecnología de la información a efectos aduaneros (DO L 323 de 10.12.2009, p. 20).

53 Convenio relativo a la asistencia mutua y la cooperación entre las administraciones aduaneras, establecido sobre la base del artículo K.3 del Tratado de la Unión Europea (DO C 24 de 23.1.1998, p. 2).

54 Aplicación del artículo 7, apartado 2, y del artículo 8, apartado 3, de la Decisión 2009/917/JAI del Consejo, de 30 de noviembre de 2009, sobre la utilización de la tecnología de la información a efectos aduaneros - listas actualizadas de autoridades competentes (13394/11 ENFOCUSTOM 85).

El SIA incluye datos personales con referencia a productos, medios de transporte, empresas, personas y mercancías, y efectivo retenidos, incautados o decomisados. Los datos personales solo pueden copiarse del SIA a otros sistemas de tratamiento de datos para gestión de riesgos o análisis operativo, a los que únicamente pueden acceder los analistas designados por los Estados miembros.

FIDE permite a las autoridades nacionales encargadas de llevar a cabo investigaciones aduaneras, cuando abren un expediente de investigación, identificar otras autoridades que pueden haber investigado a una persona o empresa determinada.

2.9. Documentos Auténticos y Falsos en Red - FADO[55]

Se trata de un sistema de archivo de imágenes informatizado que comprende documentos falsos y auténticos y se basa en tecnología de internet que permite un intercambio de información rápido y seguro entre la Secretaría General del Consejo de la Unión Europea y los verificadores de documentos en todos los Estados miembros, así como en Islandia, Noruega y en Suiza. El sistema permite una comparación en pantalla entre el documento original y el falsificado o falso. En primer lugar, contiene documentos de los Estados miembros, así como documentos de países terceros desde los que existen flujos migratorios regulares a los Estados miembros. La base de datos creada en FADO contiene los siguientes datos:

- imágenes de documentos auténticos
- información sobre técnicas de seguridad (dispositivos de seguridad)
- imágenes de documentos falsos y falsificados típicos
- información sobre técnicas de falsificación, y
- estadísticas sobre documentos falsos y falsificados detectados y usurpación de identidad

[55] Acción Común 98/700/JAI, de 3 de diciembre de 1998, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, por la que se crea un Sistema europeo de archivo de imágenes (FADO) (DO L 333 de 9.12.1998, p. 4).

El sistema utiliza líneas de datos especiales entre la Secretaría General del Consejo y los servicios centrales ubicados en los Estados miembros. Dentro de cada Estado miembro, el sistema se lee a través de una conexión segura a internet desde un servicio central. Un Estado miembro puede usar el sistema internamente en su propio territorio, lo que significa conectar distintas comisarías en sus distintos puestos de control fronterizo u otras autoridades competentes. No obstante, no existe nexo directo entre un puesto de trabajo, distinto del servicio central nacional, y el punto central en la Secretaría General.

FADO puede consultarse actualmente en 22 lenguas oficiales de la Unión Europea. Expertos en documentos introducen los documentos en cualquiera de las lenguas y los modelos de descripción se traducen automáticamente. Por tanto, los documentos están inmediatamente disponibles en todas las lenguas de apoyo. La información en texto libre adicional contenida la traducen posteriormente lingüistas especializados en la Secretaría General del Consejo.

2.10. Registro Público de Documentos Auténticos de Identidad y de Viaje en Red - PRADO

Mientras que el acceso a FADO está limitado a verificadores de documentos y uso gubernamental, el Registro Público de Documentos Auténticos de Identidad y de Viaje en Red del Consejo de la Unión Europea (PRADO) contiene un subconjunto de información FADO que se pone a disposición del público en general. La Secretaría General del Consejo de la Unión Europea publica el sitio web[56] en las lenguas oficiales de la UE por motivos de transparencia y ofrece un servicio importante a muchos usuarios en Europa, en especial a organizaciones no gubernamentales que necesitan o tienen la obligación legal de comprobar identidades.

El sitio web contiene descripciones técnicas, incluida información sobre dispositivos de seguridad, de identidad auténtica y documentos de viaje. Los expertos en documentos de los Estados miembros, Islandia, Noruega y Suiza son los encargados de seleccionar y proporcionar la información.

En PRADO, los usuarios también pueden encontrar enlaces a sitios web con información sobre números de documentos inválidos facilitados por algunos Estados miembros, así como por terceros países, y otra información relativa a control de identidad y documentos y fraude.

[56] http://www.prado.consilium.europa.eu/ (en inglés)

2.11. Sistema de Entradas y Salidas (SES)

El principal objetivo del Sistema de Entradas y Salidas[57] (SES) es mejorar la gestión de las fronteras exteriores de la Unión[58]. Registra electrónicamente el momento y el lugar de entrada y de salida de determinados nacionales de terceros países admitidos para una estancia de corta duración en el territorio de los Estados miembros, y calcula la duración de la estancia autorizada.

Además, pueden consultar el SES, únicamente con arreglo a las condiciones establecidas en el Reglamento, las autoridades policiales nacionales, con fines de prevención, detección o investigación de delitos de terrorismo y otros delitos graves.

El Reglamento establece normas estrictas sobre el acceso al EES. Asimismo, establece los derechos de acceso, rectificación, compleción, supresión y compensación de las personas, en particular el derecho de recurso judicial y la supervisión de las operaciones de tratamiento por autoridades públicas independientes. El Reglamento respeta los derechos fundamentales y observa los principios reconocidos por la Carta de los Derechos Fundamentales de la UE.

El SES está compuesto por

- un sistema central (sistema central del SES), que contiene una base de datos central informatizada de datos biométricos (impresiones dactilares e imágenes faciales) y alfanuméricos,
- una interfaz nacional uniforme en cada Estado miembro;
- una infraestructura de comunicación segura y cifrada que conecta el sistema central del SES a la interfaz nacional uniforme,
- un canal de comunicación seguro, que conecta el sistema central del SES con el sistema central del Sistema de Información de Visados (VIS) con fines de consulta.

---

[57] Reglamento (UE) 2017/2226 del Parlamento Europeo y del 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 (DO L 327 de 9.12.2017, p. 20),

[58] La Comisión determinará la fecha a partir de la cual deberá comenzar a funcionar el SES, una vez que se cumplan las condiciones establecidas en el artículo 66 del Reglamento (UE) 2017/2226.

El Reglamento determina qué autoridades de los Estados miembros están facultadas para acceder al SES con el fin de introducir, modificar, suprimir o consultar datos para los fines específicos del SES y en la medida necesaria para el desempeño de sus funciones. Todo tratamiento de datos del SES debe ser proporcionado a los objetivos que se persiguen y necesario para el desempeño del cometido de las autoridades competentes.

Las condiciones de acceso al SES para las autoridades policiales nacionales les permiten tratar los casos de sospechosos que utilizan identidades múltiples. El uso específico de los datos biométricos almacenados en el SES se justifica, a pesar de su injerencia en la intimidad del viajero, para identificar a aquellos viajeros sin documentos de viaje u otra identificación. Pero también pueden utilizarse para obtener pruebas mediante el seguimiento de las rutas de viaje de una persona sospechosa de haber cometido un delito o de una víctima de un delito.

El acceso a los datos del SES con fines policiales constituye una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de los datos de carácter personal de las personas cuyos datos se tratan en el EES. Dicho tratamiento está regulado por las disposiciones de la Directiva (UE) 2016/680 («Directiva sobre policía»)[59].

En el ejercicio de sus funciones, las autoridades policiales nacionales pueden comparar una huella dactiloscópica hallada en el lugar del delito («impresiones dactilares latentes») con los datos dactiloscópicos almacenados en el SES, cuando existen motivos razonables para presumir que el autor o la víctima figuran en el SES. No obstante, el acceso de los servicios de seguridad al SES para identificar a sospechosos, autores o víctimas desconocidos de delitos de terrorismo u otros delitos graves está supeditado a la condición de que se hayan consultado las bases de datos nacionales y se haya llevado a cabo íntegramente una búsqueda de impresiones dactilares en el marco de la Decisión 2008/615/JAI[60] del Consejo («Decisión Prüm»), o de que la consulta no se haya llevado a cabo íntegramente en el plazo de dos días a partir de su puesta en marcha.

---

[59] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2019 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),

[60] Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza (DO L 210 de 6.5.2008, p. 1).

Al igual que los procedimientos y condiciones de acceso de las autoridades policiales nacionales, los datos del SES también están a disposición de Europol en el marco de sus funciones y con sujeción a las condiciones y limitaciones establecidas en el Reglamento. Europol trata la información obtenida a partir de una consulta de datos en el SES cuando dispone de autorización del Estado miembro de origen. Dicha autorización se recabará a través de la unidad nacional de Europol de dicho Estado miembro. El Supervisor Europeo de Protección de Datos debe observar el tratamiento de los datos por parte de Europol y velar por el pleno cumplimiento de las correspondientes normas de protección de datos.

2.12. Sistema Europeo de Información y Autorización de Viajes (SEIAV)[61]

El SEIAV es un soporte para el intercambio de información en el ámbito de la gestión de las fronteras, las funciones policiales y la lucha contra el terrorismo[62]. El objeto del sistema es determinar la admisibilidad de los nacionales de terceros países exentos de visado antes de que se desplacen al espacio Schengen y lleguen a los pasos fronterizos exteriores. El SEIAV establece una autorización de viaje que es, por naturaleza, independiente de un visado, pero constituye una condición de entrada y residencia, e indica que el solicitante no supone una amenaza para la seguridad, un riesgo de inmigración ilegal ni un peligro elevado de epidemia. Las autorizaciones de viaje expedidas deben anularse o revocarse en cuanto sea patente que no se cumplen o que han dejado de cumplirse las condiciones para su expedición.

El SEIAV está compuesto por

- un sistema de información a gran escala, esto es, el sistema de información SEIAV, diseñado, desarrollado y gestionado técnicamente por la eu-LISA;

- la unidad central del SEIAV, que forma parte de la Agencia Europea de la Guardia de Fronteras y Costas;

---

61 Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se crea 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). Reglamento (UE) 2018/1241 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se modifica el Reglamento (UE) 2016/794 con objeto de establecer el Sistema Europeo de Información y Autorización de Viajes (SEIAV), DO L 236 de 19.9.2018, p. 72.

62 La Comisión determinará la fecha a partir de la cual deberá comenzar a funcionar el SEIAV, una vez que se cumplan las condiciones establecidas en el artículo 88 del Reglamento (UE) 2018/1240.

- las unidades nacionales SEIAV, encargadas de examinar las solicitudes y de decidir expedir o rechazar, anular o retirar las autorizaciones de viaje. Con este fin, han de cooperar entre ellas y con Europol para evaluar las solicitudes.

Los datos personales facilitados por el solicitante únicamente son tratados por el SEIAV a efectos de evaluar si su entrada en la Unión podría suponer una amenaza para la seguridad, un riesgo de inmigración ilegal o un peligro elevado de epidemia. Para la evaluación de riesgos, los datos personales facilitados deben compararse con los que figuran en un registro, expediente o descripción registrados en un sistema de información o base de datos de la UE (el Sistema de Información de Schengen (SIS), el Sistema de Información de Visados (VIS) el Sistema de Entradas y Salidas (SES) o Eurodac), los datos de Europol o las bases de datos de Interpol (base de datos de Interpol sobre documentos de viaje robados y perdidos –SLTD– o base de datos de Interpol de documentos de viaje asociados a notificaciones –TDAWN–). Los datos personales también deben cotejarse con la lista de alerta rápida del SEIAV y con indicadores de riesgo específicos.

El cotejo se efectúa por medios automatizados. En caso de que se produzca una «respuesta positiva» –es decir, una coincidencia entre los datos personales de la solicitud y los indicadores de riesgo específicos o los datos personales, ya sea en un expediente de registro o en una descripción contenida en los sistemas de información mencionados o en la lista de alerta rápida–, la solicitud debe ser tratada manualmente por la unidad nacional del Estado miembro responsable. Esta evaluación debe llevar a la decisión de expedir o no la autorización de viaje.

A fin de cumplir los objetivos generales del SEIAV, se tratan cantidades considerables de datos personales. El Reglamento respeta los derechos fundamentales y cumple los principios reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea. Por lo tanto, hay salvaguardas apropiadas cuyo objeto es limitar la interferencia con el derecho a la protección de la vida privada y el derecho a la protección de los datos personales a lo que estrictamente necesario y proporcionado en una sociedad democrática. Por esta misma razón, los criterios utilizados para definir los indicadores de riesgo específicos no deben basarse en ningún caso en datos personales sensibles[63].

[63] 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 (DO L 119 de 4.5.2016, p. 1).

El acceso a los datos personales del SEIAV ha de quedar limitado al personal estrictamente autorizado y en ningún caso debe utilizarse para adoptar decisiones basadas en alguna forma de discriminación. Por lo que respecta a las autoridades policiales, el tratamiento de los datos almacenados en el sistema central del SEIAV solo debe producirse en casos concretos y solo cuando sea necesario a efectos de prevención, detección o investigación de delitos de terrorismo o delitos graves. Las autoridades designadas y Europol solo deben solicitar acceso al SEIAV cuando tengan motivos fundados para pensar que dicho acceso facilitará información que les ayude en la prevención, detección o investigación de un delito de terrorismo o un delito grave.

2.13. Resumen de sistemas de información utilizados para el intercambio de información UE

Sistemas y bases de datos IT	Base jurídica	Fin	Interesados	Puesta en común de datos
Sistema de Información de Schengen de segunda generación - SIS II	Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), DO L 205 de 7.8.2007, p. 63.	• Seguridad interior • Control de fronteras • Cooperación judicial • Investigación de delito	• Ciudadanos de la UE • Nacionales de un tercer país	• Sistema de Información de Visados (VIS) • Europol • Eurojust • Interpol
	Reglamento (CE) N.º 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II), DO L 381 de 23.12.2006, p. 4.	• Denegación de entrada o estancia • Políticas de asilo, inmigración y regreso	• Nacionales de países terceros que no disfrutan de derechos de libre circulación equivalentes a los de los ciudadanos de la UE	
Europol SIE	Decisión 2009/371/JAI del Consejo, de 6 de abril de 2009, por la que se crea la Oficina Europea de Policía (Europol), artículos 11 a 13, DO L 121 de 15.5.2009, p. 37.	• Delito grave • Inmigración • Seguridad interior • Lucha antiterrorista	• Ciudadanos de la UE • Nacionales de un tercer país	• SIS II
Interpol I-24/7	Estatuto de Interpol		• Ciudadanos de la UE • Nacionales de un tercer país	• SIS II • Europol • Sistema de Información de Visados (VIS)

Interpol **Documentos de viaje extraviados/robados**	Posición Común 2005/69/JAI del Consejo relativa al intercambio de determinados datos con Interpol DO L 27 de 29.1.2005, p. 61.	• Crimen organizado e internacional • Seguridad interior	• Ciudadanos de la UE • Nacionales de un tercer país	
ECRIS	Directiva (UE) 2019/884 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por la que se modifica la Decisión Marco 2009/315/JAI del Consejo en lo que respecta al intercambio de información sobre nacionales de terceros países y al Sistema Europeo de Información de Antecedentes Penales (ECRIS) y por la que se sustituye la Decisión 2009/316/JAI del Consejo, DO L 171 de 7.6.20199, p. 143.	Procedimientos penales	• Ciudadanos de la UE • Nacionales de un tercer país	
ECRIS-TCN	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-TCN) a fin de complementar 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. Directiva (UE) 2019/884 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por la que se modifica la Decisión Marco 2009/315/JAI del Consejo en lo que respecta al intercambio de información sobre nacionales de terceros países y al Sistema Europeo de Información de Antecedentes Penales (ECRIS) y por la que se sustituye la Decisión 2009/316/JAI del Consejo, DO L 171 de 7.6.2019, p. 143.	Procedimientos penales	• Nacionales de un tercer país	• Europol • Eurojust • Fiscalía Europea

VIS	Decisión del Consejo de 8 de junio de 2004, por la que se establece el Sistema de Información de Visados (VIS) (2004/512/CE), DO L 213 de 15.6.2004, p. 5. Decisión 2008/633/JAI del Consejo 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. Decisión del Consejo por la que se establece la fecha a partir de la cual surtirá efecto la Decisión 2008/633/JAI 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 (2013/392/UE), DO L 198 de 23.7.2013, p. 45.	• Delito grave • Seguridad interior • Lucha antiterrorista	• Nacionales de un tercer país	• SIS II • Europol • Interpol

Eurodac	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.º 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 (refundición), DO L 180 de 29.06.2013, p. 1. Reglamento (UE) n.º 604/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 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, DO L 180 de 29.6.2013, p. 31.	• Inmigración • Delito grave • Seguridad interior • Lucha antiterrorista	• Nacionales de un tercer país	Europol

Registro de nombres de los pasajeros **(PNR)**	Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave, DO L 119 de 4.5.2016, p. 132.	• Delito grave • Seguridad interior • Lucha antiterrorista	• Ciudadanos de la UE • Nacionales de un tercer país	Europol
Información anticipada sobre los pasajeros (datos API)	Directiva 2004/82/CE del Consejo de 29 de abril de 2004 sobre la obligación de los transportistas de comunicar los datos de las personas transportadas, DO L 261 de 6.8.2004, p. 24.	• Control de fronteras • Inmigración	• Nacionales de un tercer país	
SEIAV	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[64], DO L 236 de 19.9.2018, p. 1. Reglamento (UE)2018/1241 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se modifica el Reglamento (UE) 2016/794 con objeto de establecer el Sistema Europeo de Información y Autorización de Viajes (SEIAV), DO L 236 de 19.9.2018, p. 72.	• Control de fronteras • Inmigración • Delito grave • Seguridad interior • Lucha antiterrorista	• Nacionales de un tercer país	• SIS • VIS • SES • Eurodac • Europol • Interpol • Lista de alerta rápida del SEIAV

[64] La Comisión determinará cuándo debe comenzar a funcionar el SEIAV, una vez que se cumplan las condiciones establecidas en el artículo 88 del Reglamento.

SES	Reglamento (UE) 2017/2225 del Parlamento Europeo y del Consejo, de 30 de noviembre de 2017, por el que se modifica el Reglamento (UE) 2016/399 en lo que respecta a la utilización del Sistema de Entradas y Salidas, DO L 327 de 9.12.2017, p. 1. Reglamento (UE) 2017/2226 del Parlamento Europeo y del 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[65], DO L 327 de 9.12.2017, p. 20.	• Gestión de las fronteras • Delito grave • Lucha antiterrorista	• Nacionales de un tercer país	• VIS • Europol • Decisión Prüm
SIC	Decisión 2009/917/JAI del Consejo, de 30 de noviembre de 2009, sobre la utilización de tecnología de la información a efectos aduaneros, DO L 323 de 10.12.2009, p. 20.	• Lucha contra el tráfico ilícito	• Ciudadanos europeos • Nacionales de un tercer país	Europol

[65] La Comisión determinará a partir de cuándo debe comenzar a funcionar el SES, una vez que se cumplan las condiciones establecidas en el artículo 66 del Reglamento.

FADO	Acción Común 98/700/JAI, de 3 de diciembre de 1998, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, por la que se crea un Sistema europeo de archivo de imágenes (FADO), DO L 333 de 9.12.1998, p. 4.	• Lucha contra los documentos falsos • Política de inmigración • Cooperación policial	• Ciudadanos europeos • Nacionales de un tercer país	

3. LEGISLACIÓN - CONTEXTO JURÍDICO, NORMAS Y DIRECTRICES RELATIVAS A LOS PRINCIPALES MÉTODOS Y SISTEMAS DE COMUNICACIÓN

3.1. Directiva de protección de datos[66]

La Directiva (UE) 2016/680 por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[67], establece normas específicas relativas a la:

- la protección de las personas físicas, sea cual fuere su nacionalidad o lugar de residencia, con respecto al tratamiento, bien por medios automáticos, bien por otro tipo de medios, de datos personales por parte de la policía u otras fuerzas y cuerpos de seguridad dentro de su ámbito de competencias, y

- el intercambio de los datos personales dentro del territorio de la Unión por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

Su objetivo es garantizar el mismo nivel de protección de las personas físicas a través de derechos jurídicamente exigibles en toda la Unión y evitar divergencias que dificulten el intercambio de datos personales entre las autoridades competentes.

Los Estados miembros transpondrán la Directiva antes del 6 de mayo de 2018. No obstante, cuando ello suponga un esfuerzo desproporcionado, podrán disponer excepcionalmente que se apliquen para el 6 de mayo de 2023 a más tardar las disposiciones de control relativas a operaciones llevadas a cabo mediante sistemas de tratamiento automatizado establecidos antes del 6 de mayo de 2016.

---

66 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).

67 Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO L 350 de 30.12.2008, p. 60). La Decisión Marco queda derogada con efecto a partir del 6 de mayo de 2018.

El término «autoridades competentes» incluye autoridades públicas tales como las autoridades judiciales, la policía u otras fuerzas y cuerpos de seguridad, así como también cualquier otro organismo o entidad a los que en virtud del Derecho del Estado miembro se haya confiado el ejercicio de la autoridad y las competencias públicas a los efectos de la presente Directiva. Las actividades de las fuerzas y cuerpos de seguridad se centran principalmente en la prevención, investigación, detección o enjuiciamiento de infracciones penales. Estas actividades también pueden incluir las actuaciones policiales en manifestaciones, grandes acontecimientos deportivos y disturbios. Entre dichas actividades también figura el mantenimiento del orden público, como labor encomendada a la policía, cuando sea necesario, para la protección y prevención frente a las amenazas para la seguridad pública y para los intereses fundamentales de la sociedad que puedan ser constitutivas de infracciones penales.

El tratamiento de datos personales a efectos que queden fuera del ámbito de las actividades mencionadas anteriormente y a efectos que los Estados miembros puedan confiar adicionalmente a las autoridades policiales, y el tratamiento de datos personales en la medida en que esté comprendido en el ámbito de aplicación del Derecho de la Unión, quedará regulado por el Reglamento (UE) 2016/679[68]. Por otra parte, la Directiva (UE) 2016/680 no abarca el tratamiento de datos en relación con actividades referentes a la seguridad nacional, las actividades de organismos y órganos que se ocupan de cuestiones de seguridad nacional o el tratamiento de datos por parte de los Estados miembros cuando efectúan actividades en relación con la política exterior y de seguridad común[69].

A efectos de la Directiva sobre protección de datos se entenderá por:

- **«datos personales»**: toda información sobre una persona física («el interesado») identificada o identificable, directa o indirectamente, en particular mediante una referencia a un nombre, un número de identificación, unos datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

  Los Estados miembros dispondrán que las autoridades competentes que realicen el tratamiento de datos diferencien claramente, si procede y siempre que sea posible, las distintas categorías de interesados, tales como a) los sospechosos, b) los condenados, c) las víctimas y d) las terceras partes involucradas en una infracción penal, como los testigos.

---

[68] 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).

[69] Capítulo 2 del título V del Tratado de la Unión Europea (TUE)

- «**Tratamiento»:** cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Los datos personales deben ser tratados lícita y lealmente, y únicamente con los fines específicos previstos en la ley. Para que sea lícito, dicho tratamiento debe ser necesario para el desempeño de una función llevada a cabo por una autoridad competente para los fines policiales mencionados anteriormente. El principio de tratamiento leal en materia de protección de datos es un concepto distinto del derecho a un «juicio imparcial», según se define en el artículo 47 de la Carta y en el artículo 6 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Los datos personales tienen que ser suficientes y pertinentes en relación con los fines para los que sean tratados.

El tratamiento de datos personales especialmente sensibles que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos para el mero fin de identificar a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física solo se permitirá cuando sea estrictamente necesario, con sujeción a las salvaguardias adecuadas para los derechos y libertades del interesado y únicamente bajo condiciones restrictivas y bien definidas.

La creación de autoridades de control nacionales que ejerzan sus funciones con plena independencia constituye un elemento esencial de la protección de las personas físicas en lo que respecta al tratamiento de sus datos. Las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas en aplicación de la Directiva y deben contribuir a su aplicación coherente en toda la Unión. La protección de los derechos y libertades de los interesados, así como la responsabilidad de las autoridades competentes nacionales y de los encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades.

La circulación de los datos personales a través de las fronteras puede obstaculizar la capacidad de las personas físicas para protegerse de la utilización o difusión ilícitas de dichos datos. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades realizadas fuera de sus fronteras. Sus esfuerzos por colaborar en el ámbito transfronterizo también pueden verse obstaculizados por la insuficiencia de las facultades preventivas o correctivas o la incoherencia de los ordenamientos jurídicos. Por tanto, es necesario fomentar una cooperación más estrecha entre las autoridades de control de la protección de datos a fin de contribuir al intercambio de información con sus homólogos extranjeros.

3.2. La «Decisión Marco sueca» (SFD)[70]

Como desarrollo del acervo de Schengen, la Decisión Marco 2006/960/JAI del Consejo («Decisión Marco sueca» - SFD) establece, en particular, las normas relativas a plazos y modelos de formularios para el intercambio de información transfronterizo[71], previa petición o espontáneamente, entre los servicios de seguridad competentes designados de los Estados miembros a efectos de:

- prevenir, detectar e investigar delitos o actividades delictivas que correspondan o sean equivalentes a los mencionados en la Orden de detención europea[72], o
- prevenir una amenaza inmediata y grave para la seguridad pública.

Las autoridades designadas están obligadas a responder en el plazo máximo de ocho horas en casos urgentes, siempre que los servicios de seguridad puedan acceder directamente a la información o inteligencia solicitada. La información puede no facilitarse cuando:

- esté en peligro la seguridad nacional,
- pueden perjudicarse investigaciones en curso,

---

70 Decisión Marco 2006/960/JAI del Consejo, de 18 de diciembre de 2006, sobre la simplificación del intercambio de información e inteligencia entre los servicios de seguridad de los Estados miembros de la Unión Europea (DO L 386 de 29.12.2006, p. 89 con corrección de errores en el DO L 75 de 15.3.2007, p. 26).

71 Véase infra el cuadro 1.

72 El doc. 8216/2/08 REV 2 contiene la versión final del manual europeo para la emisión de órdenes de detención europeas. El artículo 2 de la Decisión Marco 2002/584/JAI del Consejo sobre la Orden de detención europea establece el ámbito de esta última.

- la solicitud se refiere a un delito castigado con pena de cárcel de un año o inferior en la legislación del Estado miembro requerido,

- La autoridad judicial competente niega el acceso a la información.

Los términos «información o inteligencia» abarcan las dos categorías siguientes:

– todo tipo de información o datos en poder de los servicios de seguridad

– todo tipo información o datos en poder de autoridades públicas o entes privados, de la que puedan disponer los servicios de seguridad sin tener que utilizar medidas coercitivas

El contenido de estas categorías depende de la legislación nacional. El tipo de información disponible en cada Estado miembro se recoge en las hojas nacionales adjuntas a este manual.

Los datos se comparten con Europol en la medida en que la información o inteligencia intercambiada se refiere a un delito o actividad delictiva que sea competencia de Europol. La información y la inteligencia se procesarán con arreglo a los respectivos códigos de tratamiento de Europol. SIENA (la Aplicación de la Red de Intercambio Seguro de Informaciónde Europol) es un .soporte para el intercambio de información con arreglo a la Decisión Marco sueca

Los Estados miembros garantizan que las condiciones de intercambio de información transfronterizo no son más estrictas que las aplicables en un caso interno. Los servicios de seguridad competentes no están obligados, en particular, a solicitar la aprobación o autorización judicial previa al intercambio de información transfronterizo si la información buscada está disponible a nivel nacional sin tal aprobación o autorización. No obstante, cuando se exija una autorización judicial, la autoridad judicial aplicará, al dictar su decisión, los mismos criterios en el caso transfronterizo que si se tratara de un asunto exclusivamente interno. La información que requiera autorización judicial se indica en las fichas nacionales.

Puesto que los profesionales consideraron que el formulario tipo de solicitud era demasiado engorroso, se ha desarrollado un formulario de solicitud de información e inteligencia no obligatorio[73]. Cuando no sea posible emplear este formulario simplificado, se utilizará preferentemente otro formulario o un texto libre no estructurado.

[73] Véase infra el cuadro 2.

No obstante, estas solicitudes cumplirán en cualquier caso los requisitos del artículo 5 de la Decisión Marco sueca, y contendrán al menos los siguientes puntos obligatorios:

- información administrativa, a saber, Estado miembro requirente, autoridad requirente, fecha, número o números de referencia, Estado o Estados miembros requeridos
- si la solicitud es urgente y, en caso afirmativo, los motivos de la urgencia
- descripción de la información o inteligencia solicitada
- identidad(es) (en la medida en que se conozca) de las personas u objetos que constituyan la materia principal de la investigación criminal o de la operación de inteligencia criminal en las que se fundamenta la solicitud de la información o inteligencia (por ejemplo, descripción de los delitos y circunstancias en que se cometieron, etc.)
- fin para el que se busca la información o inteligencia
- vinculación entre el fin y la persona que es objeto de la información o inteligencia
- motivos que inducen a pensar que la información o inteligencia se encuentran en el Estado miembro requerido
- restricciones a la utilización de la información que figura en la solicitud («códigos de tratamiento»)

El Estado miembro requirente puede elegir alguno de los canales existentes para la comunicación policial internacional (SIRENE, Europol, Interpol y puntos de contacto bilaterales). El Estado miembro que responde normalmente utiliza el mismo cauce utilizado para la solicitud. Sin embargo, cuando el Estado miembro requerido responda, por motivos legítimos, a través de otro cauce, el servicio requirente será informado del cambio. La lengua utilizada para la solicitud y la entrega de información será la aplicable para el cauce utilizado.

Se adjunta a este manual un resumen de los **acuerdos bilaterales o de otro tipo existentes**.

Cuadro 1

ANEXO A

INTERCAMBIO DE INFORMACIÓN EN VIRTUD DE LA DECISIÓN MARCO 2006/960/JAI DEL CONSEJO
FORMULARIO QUE UTILIZARÁ EL ESTADO MIEMBRO REQUERIDO EN CASO DE
TRANSMISIÓN/RETRASO/DENEGACIÓN DE INFORMACIÓN

El presente formulario se utilizará para transmitir la información y/o inteligencia requerida, para informar a la autoridad requirente de la imposibilidad de cumplir el plazo normal, de la necesidad de presentar la solicitud a la autorización de una autoridad judicial, o bien de la denegación de transmisión de la información.

El presente formulario podrá utilizarse más de una vez durante el procedimiento (p. ej., si la solicitud debe presentarse primero a una autoridad judicial y luego se pone de manifiesto que la ejecución de la solicitud debe denegarse).

Autoridad requerida (nombre, dirección, teléfono, fax, correo electrónico, Estado miembro):	
Datos del funcionario responsable (facultativo):	
Número de referencia de la presente respuesta:	
Fecha y número de referencia de la respuesta anterior:	
Respondiendo a la siguiente autoridad requirente:	
Fecha y hora de la solicitud:	
Número de referencia de la solicitud:	

Plazo normal con arreglo al artículo 4 de la Decisión marco 2006/960/JAI		
El delito está recogido en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI y La información o inteligencia solicitada se conserva en una base de datos a la que tiene acceso directo un servicio de seguridad en el Estado miembro requerido	La solicitud es urgente	➔ ❑ 8 horas
	La solicitud no es urgente	➔ ❑ 1 semana
Demás casos		➔ ❑ 14 días

Información transmitida de acuerdo con la Decisión marco 2006/960/JAI : Información e inteligencia facilitada
1. La utilización de la información o de la inteligencia facilitada ❑ Únicamente se autorizará para los fines para los que se haya facilitado o para prevenir una amenaza grave e inminente a la seguridad pública; ❑ Se autorizará asimismo a otros efectos, sin perjuicio de las siguientes condiciones (facultativo):
2. Fiabilidad de la fuente ❑ Fiable ❑ Fiable en general ❑ No fiable ❑ No puede evaluarse
3. Exactitud de la información o inteligencia ❑ Segura ❑ Certificada por la fuente ❑ Rumores confirmados ❑ Rumores no confirmados

4. Los resultados de la investigación criminal o de la operación de inteligencia criminal que haya originado el intercambio de información e inteligencia deben comunicarse a la autoridad transmisora

❑ Sí
❑ No

5. En caso de intercambio espontáneo: motivos que permitan creer que la información o inteligencia podrían contribuir a la detección, prevención o investigación de los delitos enumerados en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI:

RETRASO – No es posible responder en el plazo aplicable previsto en el artículo 4 de la Decisión marco 2006/960/JAI

No es posible facilitar la información o inteligencia en el plazo indicado por los siguientes motivos:

Es probable que se pueda facilitar dentro de:

❑ 1 día ❑ 2 días ❑ 3 días
❑ ... semanas
❑ 1 mes

❑ Se ha solicitado la autorización de una autoridad judicial.
Se espera que el procedimiento que lleva a la concesión/denegación de la autorización dure ... semanas

DENEGACIÓN – La información o inteligencia
❑ no ha podido facilitarse y solicitarse en el plano nacional, o
❑ no puede facilitarse por uno o varios de los siguientes motivos:

A – Motivo relacionado con un control judicial que impide la transmisión o requiere recurrir a la asistencia jurídica mutua

❑ la autoridad judicial competente no ha autorizado el acceso y el intercambio de información o inteligencia

❑ la información o inteligencia solicitada se obtuvo previamente mediante medidas coercitivas y la legislación nacional no permite su comunicación

❑ la información o inteligencia no está en posesión

- de un servicio de seguridad; o
- de autoridades públicas o entidades privadas de un modo que permita a un servicio de seguridad disponer de ella sin la adopción de medidas coercitivas

❑ B – La comunicación de la información o inteligencia solicitada perjudicaría intereses esenciales de seguridad nacional o comprometería el éxito de una investigación en curso o de una operación de inteligencia criminal o la seguridad de personas, o resultaría claramente desproporcionada o irrelevante respecto de los fines para los que se ha solicitado.

En caso de utilizar la casilla A o B, indique, si lo considera necesario, información adicional o los motivos (...) de denegación (facultativo):

❑ D – La autoridad requerida ha decidido denegar la ejecución debido a que la solicitud se refiere, en la legislación del Estado miembro requerido, al siguiente delito (especifique la naturaleza del delito y su tipificación jurídica) ..... castigado con pena de prisión igual o inferior a un año.

❑ E – La información o inteligencia solicitada no está disponible.

❑ F – La información o inteligencia solicitada se ha obtenido de otro Estado miembro o de un tercer país y está sometida a la regla de la especialidad, y dicho Estado miembro o tercer país no ha dado su consentimiento para la transmisión de la información o inteligencia.

ANEXO B

INTERCAMBIO DE INFORMACIÓN EN VIRTUD DE LA DECISIÓN MARCO 2006/960/JAI DEL CONSEJO
FORMULARIO DE SOLICITUD DE INFORMACIÓN E INTELIGENCIA QUE UTILIZARÁ
EL ESTADO MIEMBRO REQUIRENTE

El presente formulario se utilizará cuando se solicite información e inteligencia en virtud de la Decisión marco 2006/960/JAI

I – Información administrativa

Autoridad requirente (nombre, dirección, teléfono, fax, correo electrónico, Estado miembro):	
Datos del funcionario responsable (facultativo):	
Al Estado miembro siguiente:	
Fecha y hora de la presente solicitud:	
Número de referencia de la presente solicitud:	

Solicitudes anteriores				
❑ Es la primera solicitud sobre este asunto				
❑ Se han presentado anteriormente las siguientes solicitudes para este mismo asunto				
Solicitud(es) anterior(es)			Respuesta(s)	
	Fecha	Número de referencia (en el Estado miembro requirente)	Fecha	Número de referencia (en el Estado miembro requerido)
1.				
2.				
3.				
4.				

Si la solicitud se remite a más de una autoridad del Estado miembro requerido, indicar todos los canales utilizados:	
❑ Funcionario de enlace en Europol/UNE	❑ Para información ❑ Para ejecución
❑ Interpol/OCN	❑ Para información ❑ Para ejecución
❑ Sirene	❑ Para información ❑ Para ejecución
❑ Funcionario de enlace	❑ Para información ❑ Para ejecución
❑ Otros (especificar):	❑ Para información ❑ Para ejecución
Si la misma solicitud se remite a otro Estado miembro, indicar de qué Estados miembros se trata y los canales utilizados (facultativo)	

II – Plazos

Recordatorio: plazos con arreglo al artículo 4 de la Decisión marco 2006/960/JAI

A – El delito está recogido en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI

y

La información o inteligencia solicitada se conserva en una base de datos a la que tiene acceso directo un servicio de seguridad

→ La solicitud es urgente → Plazo: 8 horas con posibilidad de aplazamiento

→ La solicitud no es urgente → Plazo: 1 semana

B – Demás casos: plazo: 14 días

❑ **Se solicita tratar con urgencia**
❑ **NO se solicita tratar con urgencia**
Motivos de la urgencia (p. ej.: sospechosos detenidos, el asunto debe presentarse ante un tribunal antes de una fecha concreta)
Información o inteligencia solicitada

Tipos De Delito O Actividad Delictiva Investigados
Descripción de las circunstancias de la comisión del delito o delitos, incluido el momento, lugar y grado de participación en ellos de la persona objeto de la información o inteligencia solicitada:

Naturaleza del delito o delitos

A – Aplicación de los apartados 1 o 3 del artículo 4 de la Decisión marco 2006/960/JAI

❑ A.1. El delito está penado con una pena máxima privativa de libertad de al menos tres años en el Estado miembro requirente
Y
A.2. El delito es uno (o varios) de los siguientes:

- ❑ pertenencia a organización delictiva
- ❑ terrorismo
- ❑ trata de seres humanos
- ❑ explotación sexual de menores y pornografía infantil
- ❑ tráfico ilícito de estupefacientes y sustancias psicotrópicas
- ❑ tráfico ilícito de armas, municiones y explosivos
- ❑ corrupción
- ❑ fraude, incluido el que afecte a los intereses financieros de las Comunidades Europeas con arreglo al Convenio de 26 de julio de 1995 relativo a la protección de los intereses financieros de las Comunidades Europeas
- ❑ atraco organizado o a mano armada
- ❑ tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte
- ❑ estafa
- ❑ chantaje y extorsión
- ❑ falsificación y piratería de productos
- ❑ falsificación de documentos administrativos y tráfico de documentos falsos
- ❑ falsificación de medios de pago
- ❑ tráfico ilícito de sustancias hormonales y otros factores de crecimiento
- ❑ blanqueo del producto del delito
- ❑ falsificación de moneda, con inclusión del euro
- ❑ delito informático
- ❑ delitos contra el medio ambiente, incluido el tráfico ilícito de especies animales protegidas y de especies y variedades vegetales protegidas
- ❑ ayuda a la entrada y a la estancia irregulares
- ❑ homicidio, lesiones graves
- ❑ tráfico ilícito de órganos y tejidos humanos
- ❑ secuestro, detención ilegal y toma de rehenes
- ❑ racismo y xenofobia
- ❑ tráfico ilícito de materiales radiactivos o sustancias nucleares
- ❑ tráfico de vehículos robados
- ❑ violación
- ❑ incendio provocado
- ❑ delitos incluidos en el ámbito de competencia de la Corte Penal Internacional
- ❑ secuestro de aeronaves y buques
- ❑ sabotaje

→ Por consiguiente, el delito está recogido en el artículo 2, apartado 2, de la Decisión marco 2002/584/JAI. Por tanto, el artículo 4, apartado 1 (casos urgentes) y el artículo 4, apartado 3 (casos no urgentes) de la Decisión marco …/…/JAI se aplican en relación con los plazos que se han de cumplir para responder a la presente solicitud.

❑ B – El delito o delitos no están recogidos en la letra A.
- En tal caso, descripción del delito o delitos:

Fin para el que se solicita la información o inteligencia

Vinculación entre el fin para el cual se solicita la información o inteligencia y la persona objeto de la información o inteligencia

Identidad o identidades (en la medida en que se conozcan) de la persona o personas objeto principal de la investigación criminal o de la operación de inteligencia criminal en las que se fundamenta la solicitud de la información o inteligencia

Motivos que inducen a pensar que la información o inteligencia se encuentran en el Estado miembro requerido

Restricciones a la utilización de la información que figura en la solicitud con fines distintos de aquellos para los que se facilitó o para prevenir una amenaza inminente y grave para la seguridad pública

❑utilización autorizada
❑utilización autorizada, a condición de que no se mencione su procedencia
❑utilización no autorizada salvo autorización de quien la transmite
❑utilización no autorizada

Cuadro 2

SOLICITUD DE INFORMACIÓN E INTELIGENCIA

Al amparo de la Decisión Marco 2006/960/JAI

I - Información administrativa

Estado miembro requirente	
Autoridad requirente (nombre, dirección, teléfono, fax, correo electrónico):	
Datos del funcionario responsable *(facultativo)***:**	
Fecha y hora de la presente solicitud:	
Número de referencia de la presente solicitud:	
Números de referencia anteriores	

Estado o Estados miembro requeridos:		
Cauce		
☐Funcionario de enlace en Europol/UNE	☐Para información	☐Para ejecución
☐Interpol/OCN	☐Para información	☐Para ejecución
☐OFICINAS SIRENE	☐Para información	☐Para ejecución
☐Funcionario de enlace	☐Para información	☐Para ejecución
☐Otros (especifíquese):	☐Para información	☐Para ejecución

II - Urgencia

Se solicita tratar con urgencia	☐Sí ☐No
Motivos de la urgencia (p. ej.: sospechosos detenidos, el asunto debe presentarse ante un tribunal antes de una fecha concreta): Aplicación del artículo	
El delito está recogido en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI relativa a la orden de detención europea	☐Sí ☐No

III - Fin

Tipos de delito o actividad(es) delictiva(s) investigados
Descripción de: - las circunstancias de la comisión de los delitos (por ejemplo, el momento, lugar y grado de participación en ellos de la persona objeto de la información o inteligencia solicitada) - motivos que inducen a pensar que la información o inteligencia se encuentran en el Estado miembro requerido, - vinculación entre el fin para el cual se solicita la información o inteligencia y la persona objeto de la misma
☐solicitud de utilización de la información como prueba cuando así lo permita la legislación nacional *(facultativo)*

IV - Tipo de información

Identidad(es) (en la medida en que se conozca) de las personas u objetos	
Persona	Objeto
Apellidos: Apellidos de nacimiento: Nombre: Fecha de nacimiento Lugar de nacimiento Sexo: ☐masculino ☐femenino ☐desconocido Nacionalidad: Información adicional:	Número de serie del arma: Número de documento: Otro número de identificación o denominación: Número de matrícula del vehículo: Número de identificación del vehículo (NIV): Tipo de documentos: Datos de contacto de la empresa (teléfono, -correo electrónico, dirección postal, dirección internet, etc.): Información adicional:

Información o inteligencia solicitada		
Persona	Vehículo	Otros
☐ verificación de la identidad ☐ investigación en bases de datos ☐ localización de la dirección/lugar de estancia	☐ datos completos de identificación ☐ identificación del propietario ☐ identificación del conductor ☐ investigación en bases de datos	☐ identificación de la empresa ☐ investigación de la empresa en bases de datos ☐ investigación de los documentos en bases de datos ☐ identificación del número de teléfono/fax ☐ identificación del titular de la dirección de correo electrónico ☐ investigación de la dirección ☐ investigación de armas ☐ ruta o vía de obtención de las armas
Otros:		

V - Códigos de tratamiento

Restricciones a la utilización de la información que figura en la solicitud con fines distintos de aquellos para los que se facilitó o para prevenir una amenaza inminente y grave para la seguridad pública
☐ para fines policiales únicamente; no utilizable en procedimientos judiciales ☐ consultar al proveedor de la información antes de utilizarla

3.3. Schengen - Intercambio de datos del SIS II y no pertenecientes al SIS II

El Acuerdo de Schengen firmado el 14 de junio de 1985 se completó en 1990 con el Convenio de aplicación del Acuerdo de Schengen (el «CAS»)[74] que creó el espacio Schengen mediante la abolición de los controles fronterizos dentro del Espacio Schengen, disposiciones comunes sobre visados y cooperación policial y judicial. El CAS establece un requisito general para la cooperación policial y para que las autoridades policiales correspondientes intercambien información dentro de los límites de sus respectivos ordenamientos jurídicos nacionales.

Con la entrada en vigor del Tratado de Ámsterdam en 1999, las medidas de cooperación hasta entonces en el marco de Schengen se integraron en el marco jurídico de la Unión Europea y los asuntos relacionados con Schengen se tratan ahora en los órganos legislativos de la UE. El Protocolo Schengen adjunto al Tratado de Ámsterdam establece acuerdos detallados para este proceso de integración.

El Sistema de Información de Schengen (SIS) se creó en virtud de las disposiciones del título IV del Convenio de 19 de junio de 1990. Constituye un instrumento esencial para la aplicación del acervo de Schengen y constituye además una medida destinada a compensar la ausencia de controles en las fronteras interiores de personas dentro del espacio Schengen mediante un instrumento de intercambio de información entre autoridades competentes.

El hecho de que el marco jurídico que rige el SIS esté compuesto actualmente por dos instrumentos independientes, a saber un Reglamento relativo a la aplicación del SIS en las fronteras y una Decisión del Consejo relativa a la cooperación policial, no influye en el hecho de que el SIS represente un sistema de información único.

---

[74] Convenio de aplicación del Acuerdo de Schengen, de 14 de junio de 1985, entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, DO L 239 de 22.9.2000, p. 19.

Legislación

Reglamento (CE) n.º 1987/2006 del Parlamento Europeo y del Consejo, de 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (DO L 381 de 28.12.2006, p. 4).

Decisión 2007/533/JAI del Consejo, de 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SIS II) (DO L 205 de 7.8.2007, p. 63).

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 de 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 modifica los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).

Disposiciones fundamentales

El Sistema de Información de Schengen (SIS) es un sistema tanto de cooperación policial como de control fronterizo y un soporte para la cooperación operativa entre autoridades policiales y autoridades judiciales en asuntos penales. Una selección de funcionarios policiales, guardias de fronteras, funcionarios de aduanas y autoridades judiciales y de visados en todo el espacio Schengen puede consultar el SIS.[75]

El sistema de Información de Schengen de segunda generación («SIS II») está actualmente en funcionamiento en 26 Estados miembros de la UE, así como en cuatro países fuera de la UE asociados a la cooperación Schengen: Islandia, Noruega, Suiza y Liechtenstein.

[75] La lista consolidada de autoridades nacionales competentes en la que se especifica los datos que puede buscar cada autoridad y los fines de dicha búsqueda se publica anualmente en el *Diario Oficial de la UE* con arreglo a lo dispuesto en el artículo 31, apartado 8, del Reglamento SIS y en el artículo 46, apartado 8, de la Decisión SIS II.

- En lo que respecta a la cooperación policial, el Reino Unido e Irlanda solicitaron autorización para participar en ella, pero únicamente se autorizó al Reino Unido en 2015, y de forma provisional, a cargar datos en tiempo real de dicha parte del SIS[76] a modo de primer paso para la realización de una evaluación previa a una Decisión definitiva «sobre la ejecución». El Reino Unido e Irlanda no participan en la ejecución del SIS con fines de control fronterizo.

- Bulgaria, Rumanía[77] y Croacia[78] aplican las disposiciones del acervo de Schengen en materia de cooperación policial y control fronterizo. Se les ha proporcionado acceso al SIS en tiempo real con el fin de evaluar la correcta aplicación de las disposiciones del acervo de Schengen relativas al SIS. Tan pronto como estas evaluaciones hayan finalizado de forma satisfactoria, otra Decisión del Consejo distinta fijará una fecha para suprimir los controles en las fronteras interiores. Hasta dicha fecha se mantendrán algunas restricciones sobre el uso del SIS.

- Chipre todavía no tiene acceso al SIS.

Los datos del SIS II pueden buscarse en línea (sujeto a normas estrictas en materia de protección de datos) las 24 horas del día y los 7 días de la semana a través de las Oficinas SIRENE, en los puntos de control fronterizo y en los consulados en el exterior. Los datos se conocen como descripciones, al ser una descripción un conjunto de datos que permite a las autoridades identificar **personas**, es decir, ciudadanos europeos y ciudadanos que no son de la UE, u **objetos**, con vistas a emprender las acciones pertinentes para luchar contra la delincuencia y la inmigración irregular.

El personal de Europol específicamente autorizado tiene derecho, en el ámbito de su mandato, a acceder y buscar datos introducidos en el SIS II y puede pedir más información al Estado miembro de que se trate.

Los miembros nacionales de Eurojust y sus asistentes tienen derecho, en el ámbito de su mandato, a acceder y buscar datos introducidos en el SIS II.

---

[76] Decisión de Ejecución (UE) 2015/215 del Consejo, de 10 de febrero de 2015, sobre la puesta en vigor de las disposiciones del acervo de Schengen relativas a la protección de datos y sobre la puesta en vigor provisional de parte de las disposiciones del acervo de Schengen relativas al Sistema de Información de Schengen por parte del Reino Unido de Gran Bretaña e Irlanda del Norte (DO L 36 de 12.2.2015, p. 8).

[77] Decisión 2010/365/UE del Consejo, de 29 de junio de 2010, relativa a la aplicación de las disposiciones del acervo de Schengen sobre el Sistema de Información de Schengen en la República de Bulgaria y Rumanía (DO L 166 de 1.7.2010, p. 17).

[78] Decisión (UE) 2017/733 del Consejo, de 25 de abril de 2017, sobre la aplicación de las disposiciones del acervo de Schengen relativas al Sistema de Información de Schengen en la República de Croacia (DO L 108 de 26.4.2017, p. 31).

Con arreglo al artículo 47 del Convenio, funcionarios de enlace destinados en autoridades policiales en otros Estados Schengen o en países terceros se encargan del intercambio de información con arreglo a:

- El artículo 39, apartados 1, 2 y 3 con arreglo a la legislación nacional a efectos de prevenir y detectar delitos penales;

- El artículo 46, incluso por iniciativa propia, para prevenir delitos contra el orden público y la seguridad o amenazas a los mismos.

Cabe destacar que las disposiciones del artículo 39, apartados 1, 2 y 3 y del artículo 46, en la medida en que se refieren al intercambio de información e inteligencia relativa a delitos graves, se sustituyen por las de la Decisión Marco 2006/960/JAI del Consejo, («la Decisión Marco sueca»). Con todo, las disposiciones del artículo 39, apartados 1, 2 y 3 y del artículo 46 siguen siendo aplicables a delitos castigados con penas de cárcel inferiores a doce meses.

3.4. Europol

Legislación

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, aplicable desde el 1 de mayo de 2017).

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 de 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 modifica los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).

Disposiciones fundamentales

El objetivo de Europol es apoyar y reforzar la actuación de las autoridades competentes de los Estados miembros encargadas de prevenir y combatir delitos, y su cooperación mutua en la prevención y lucha contra el crimen organizado, el terrorismo y demás formas de delitos graves que afectan a dos o más Estados miembros. A tal efecto, Europol recoge, almacena, procesa, analiza e intercambia información e inteligencia criminal.

Cada Estado miembro designa una unidad nacional de Europol (UNE) que funciona como órgano de enlace entre Europol y las autoridades competentes de los Estados miembros. Las UNE realizan funciones relacionadas con la difusión de información e inteligencia pertinente. Cada unidad nacional envía al menos un funcionario de enlace que constituye la oficina de enlace nacional en Europol y representa los intereses de la unidad nacional. Los funcionarios de enlace tienen funciones de difusión de información entre, por una parte, los Estados miembros y Europol y, por otra, bilateralmente entre otros países. Estos intercambios bilaterales pueden abarcar delitos dentro del mandato de Europol.

El Reglamento Europol introduce un nuevo concepto para el tratamiento de datos, que suele denominarse modelo integrado de gestión de datos. El modelo integrado de gestión de datos puede definirse como la posibilidad de utilizar información relacionada con la comisión de delitos para múltiples objetivos operativos conforme a las indicaciones del propietario de los datos, lo que posibilita su gestión y tratamiento de forma integrada y tecnológicamente neutra. Con arreglo a la Decisión del Consejo sobre Europol, el tratamiento de datos se estructuraba en torno a sistemas. El Reglamento Europol ya no hace referencia a los sistemas; en su lugar, estipula que debe indicarse la finalidad del tratamiento de datos. Para facilitar una transición gradual, los usuarios pueden seguir trabajando con los sistemas existentes de un modo que sea compatible con el nuevo marco jurídico.

La unidad nacional se encarga de comunicar con el Sistema de información de Europol (SIE) utilizado para tratar los datos necesarios para desempeñar las funciones de Europol. La unidad nacional, los funcionarios de enlace y el personal de Europol debidamente autorizado tienen derecho a introducir datos en los sistemas y recuperar datos de ellos. En términos generales se considera que la información introducida en el SIE se proporciona con el objetivo de efectuar controles cruzados (artículo 18, apartado 2, letra a) del Reglamento) y análisis estratégicos o temáticos (artículo 18, apartado 2, letra b) del Reglamento).

3.5. Interpol

Legislación

Estatuto de Interpol[79]

Normas aplicables al tratamiento de información[80]

Normas sobre control de información y acceso a expedientes de Interpol

Disposiciones fundamentales

La misión de Interpol es facilitar la cooperación policial internacional para prevenir y luchar contra la delincuencia mediante una cooperación e innovación intensificadas en materia policial y de seguridad. Se actúa dentro de los límites de las legislaciones vigentes en los Estados miembros y con el espíritu de la Declaración Universal de Derechos Humanos. Cada uno de los 190 Estados miembros mantiene una Oficina Central Nacional (OCN) con personal propio elegido entre sus funcionarios policiales muy entrenados.

El Estatuto de Interpol es un acuerdo internacional que confirma, en calidad de miembros, los gobiernos de los países que participaron en su adopción en 1956 y establece el procedimiento de solicitud de adhesión a Interpol para países que no eran miembros en 1956.

Como principal documento jurídico, el Estatuto presenta los objetivos y funciones de Interpol. Establece el mandato de la organización para velar por una cooperación lo más amplia posible entre todas las autoridades policiales y suprimir delitos de derecho común.

Además del Estatuto, una serie de textos fundamentales conforman el marco jurídico de Interpol. Se establecieron varios niveles de control para garantizar el cumplimiento de las normas. Estos se refieren a controles por las Oficinas Centrales Nacionales (OCN), la Secretaría General y un órgano de supervisión independiente conocido como la Comisión de control de expedientes de Interpol.

[79] https://www.interpol.int/es/Quienes-somos/Marco-juridico/Documentos-juridicos
[80] https://www.interpol.int/es/Quienes-somos/Marco-juridico/Documentos-juridicos

3.6. Funcionarios de enlace

Legislación

Convenio de aplicación del Acuerdo de Schengen (CAS) de 19 de junio de 1990, artículo 47[81].

Decisión 2003/170/JAI del Consejo, de 27 de febrero de 2003, relativa al uso conjunto de los funcionarios de enlace destinados en el extranjero por parte de los servicios policiales de los Estados miembros[82]

Decisión 2006/560/JAI del Consejo, de 24 de julio de 2006, por la que se modifica la Decisión 2003/170/JAI relativa al uso conjunto de los funcionarios de enlace destinados en el extranjero por parte de los servicios policiales de los Estados miembros[83]

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, aplicable desde el 1 de mayo de 2017).

Decisión 2008/615/JAI del Consejo sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza (DO L 210 de 6.8.2008, p. 1).

Acuerdos bilaterales

Disposiciones fundamentales

El artículo 47 del CAS dispone que los Estados miembros podrán suscribir acuerdos bilaterales que permitan el destino provisional, por un período determinado o indeterminado, de funcionarios de enlace de un Estado [miembro] en servicios de policía de otro Estado [miembro]. Los funcionarios de enlace no son competentes para ejecutar ninguna medida policial y el artículo 47 especifica que estas comisiones de servicio están destinadas a reforzar y acelerar la cooperación, en especial prestando asistencia:

a) en forma de intercambio de informaciones para luchar de forma tanto preventiva como represiva contra la criminalidad

---

81 Convenio de aplicación del Acuerdo de Schengen (CAS) de 19 de junio de 1990 (DO L 239 de 22.9.2000, p. 19).

82 Decisión 2003/170/JAI del Consejo, de 27 de febrero de 2003 (DO L 67 de 12.3.2003, p. 27).

83 Decisión 2006/560/JAI del Consejo, de 24 de julio de 2006 (DO L 219 de 10.8.2006, p. 31).

b) ejecutando las peticiones de cooperación policial y judicial en materia penal

c) a las autoridades encargadas de la vigilancia de las fronteras exteriores en el ejercicio de su cometido.

Más información sobre estas comisiones de servicio puede encontrarse en el «Manual sobre fútbol»[84] y en la recomendación del Consejo, de 6 de diciembre de 2007, relativa a un manual para las autoridades policiales y de seguridad sobre cooperación en eventos importantes de dimensión internacional[85].

La disposición del CAS según la cual los funcionarios de enlace nacionales también pueden representar los intereses de uno o varios otros Estados miembros se ha desarrollado en la Decisión del Consejo relativa al uso conjunto de los funcionarios de enlace destinados en el extranjero por parte de los servicios policiales de los Estados (modificada en 2006). También se ha previsto la mejora de la cooperación entre funcionarios de enlace de diferentes Estados miembros en su lugar de destino. En distintos foros se destacó que era preciso fomentar esta cooperación.

Con arreglo al Reglamento Europol, cada Estado miembro designa una unidad nacional (UNE) que funciona como órgano de enlace entre Europol y las autoridades competentes de los Estados miembros encargadas de prevenir y luchar contra los delitos penales. Las UNE realizan funciones relacionadas con la difusión de información e inteligencia pertinente. Cada unidad nacional envía al menos un funcionario de enlace que constituye la oficina de enlace nacional en Europol y representa los intereses de la unidad nacional. Los funcionarios de enlace tienen funciones de difusión de información entre, por una parte, la unidad nacional y Europol y, por otra, bilateralmente entre otras unidades nacionales. Estos intercambios bilaterales pueden abarcar delitos dentro del mandato de Europol.

La Decisión 2008/615/JAI del Consejo («Decisión Prüm») establece en los artículos 17 y 18 el envío de funcionarios nacionales a efectos de mantener el orden público y la seguridad, y prevenir delitos penales.

---

84 Resolución del Consejo de 3 de junio de 2010 relativa a un manual actualizado de recomendaciones para la cooperación policial internacional y de medidas de prevención y lucha contra la violencia y los desórdenes relacionados con los partidos de fútbol de dimensión internacional en los que se vea afectado al menos un Estado miembro (DO C 165 de 24.6.2010, p. 1),

85 DO C 314 de 22.12.2007, p. 4.

3.7. Intercambio de datos Prüm

Legislación

- Decisión 615/2008/JAI del Consejo de 23 de junio de 2008 sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza

- Decisión 2008/616/JAI del Consejo de 23 de junio de 2008 relativa a la ejecución de la Decisión 2008/615/JAI sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delincuencia transfronteriza, (DO L 210 de 6.8.2008).

Disposiciones fundamentales

Los Estados miembros se conceden recíprocamente acceso en línea transfronterizo a datos de referencia de determinados archivos de análisis del ADN y a sistemas automáticos de identificación dactilar (SAID), así como a datos sobre registro de vehículos (DMV) (véase el capítulo 2 de la Decisión 2008/615/JAI del Consejo).

Se designarán PCN específicos en cada Estado miembro. Se tendrán en cuenta debidamente las disposiciones sobre protección y seguridad de los datos en la legislación nacional. La comparación automatizada de perfiles biométricos anónimos está basada en un sistema de respuesta positiva / falta de respuesta positiva, salvo en caso de DMV en que los datos del propietario/titular buscados son para la devolución automática.

En caso de concordancia biométrica, el PCN del Estado miembro que inicia una búsqueda recibe, en un proceso automático, los datos de referencia respecto a los que hubo una concordancia.

Otros datos personales específicos adicionales y nueva información relativa a los datos de referencia podrán entonces pedirse a través de procedimientos de asistencia mutua, incluidos los adoptados con arreglo a la «Decisión Marco sueca».

El suministro de tales datos suplementarios se rige por la legislación nacional, incluidas las normas sobre asistencia jurídica, del Estado miembro solicitado. Se entiende que el suministro de datos personales requiere un nivel adecuado de protección de datos por parte del Estado miembro receptor.[86]

Para prevenir delitos penales y en aras de mantener el orden público y la seguridad en acontecimientos importantes con una dimensión transfronteriza, los Estados miembros pueden, tanto previa petición como por iniciativa propia, suministrarse recíprocamente datos personales y no personales. A tal fin, se designarán puntos de contacto nacionales específicos (PCN) (véase el capítulo 3 de la Decisión 2008/615/JAI del Consejo).

Para prevenir delitos terroristas, los Estados miembros pueden suministrarse recíprocamente datos personales en determinadas circunstancias. A tal fin, se designarán puntos de contacto nacionales específicos (véase el capítulo 4 de la Decisión 2008/615/JAI del Consejo).

3.8. Sistema de Información de Visados (VIS)

Legislación

Decisión del Consejo de 8 de junio de 2004 por la que se establece el Sistema de Información de Visados (VIS) (2004/512/CE) (DO L 213 de 15.6.2004, p. 5).

Decisión 2013/392/UE del Consejo por la que se establece la fecha a partir de la cual surtirá efecto la Decisión 2008/633/JAI 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 198 de 23.7.2013, p. 45)[87].

---

[86] La Decisión 2008/615/JAI del Consejo cumple el nivel de protección previsto para el tratamiento de datos personales en el Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, el Protocolo adicional al Convenio, de 8 de noviembre de 2001, y los principios de la Recomendación n.º R(87) 15 del Consejo de Europa dirigida a regular la utilización de datos de carácter personal en el sector de la policía.

[87] El 16 de abril de 2015, el Tribunal de Justicia Europeo anuló la Decisión 2013/392/UE del Consejo, de 22 de julio de 2013, por la que se establece la fecha a partir de la cual surtirá efecto la Decisión 2008/633/JAI 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. Con todo, el Tribunal declaró que los efectos de la Decisión 2013/392 debían mantenerse hasta la entrada en vigor de un nuevo acto que la sustituya.

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 de 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 modifica los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).

Disposiciones fundamentales

El VIS es un sistema que permite a las autoridades nacionales competentes introducir y actualizar datos de visados de corta duración (los denominados «visados Schengen») y consultarlos electrónicamente. Está basado en una configuración centralizada y compuesto por un sistema de información central, el Sistema de Información de Visados central (CS-VIS), una interfaz nacional en cada Estado miembro (NI-VIS), y la infraestructura de comunicación entre CS-VIS y NI-VIS. La Decisión 2008/633/JAI permite utilizar el VIS para prevenir, detectar e investigar los delitos de terrorismo y otros delitos graves. Permite acceder al VIS a las autoridades policiales designadas de los países del espacio Schengen –por ejemplo, las autoridades encargadas de la lucha contra el terrorismo o contra delitos graves como el tráfico de drogas o la trata de seres humanos– y a Europol. Una vez que se cumplen todas las condiciones de acceso, las autoridades nacionales designadas deben seguir un procedimiento para acceder al VIS.

En mayo de 2018, la Comisión presentó una propuesta legislativa por la que se modificaba el Reglamento VIS, con el fin, entre otras cosas, de garantizar la interoperabilidad entre otras bases de datos en el ámbito de la Justicia y los Asuntos de Interior. La propuesta también incorpora y desarrolla las normas para el acceso de las autoridades policiales al VIS, y deroga la Decisión 2008/633/JAI.

No se espera que el VIS mejorado sea operativo antes de finales de 2021.

3.9. Eurodac

Legislación

El sistema europeo automatizado para la comparación de impresiones dactilares (Eurodac) es en origen un sistema informático para facilitar la aplicación efectiva del Convenio de Dublín. El Convenio de Dublín, firmado el 15 de junio de 1990, fue sustituido por el Reglamento (CE) n.º 343/2003 del Consejo, de 18 de febrero de 2003, por el que se establecen los criterios y mecanismos de determinación del Estado miembro responsable del examen de una solicitud de asilo presentada en uno de los Estados miembros por un nacional de un tercer país.

Posteriormente a las modificaciones introducidas en los Reglamentos relativos a Eurodac, estas fueron refundidas en el

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.º 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 (refundición) (DO L 180 de 29.6.2013, p. 1).

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 de 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 modifica los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).

Disposiciones fundamentales

El Reglamento n.º 603/2013 establece el objetivo de Eurodac y define las condiciones para acceder a los datos de Eurodac por las autoridades policiales nacionales designadas y por Europol a efectos de prevención, detección o investigación de delitos terroristas[88] o de otros delitos penales graves[89].

3.10. Nápoles II

Legislación

Acto del Consejo, de 18 de diciembre de 1997, por el que se celebra, sobre la base del artículo K.3 del Tratado de la Unión Europea, el Convenio relativo a la asistencia mutua y la cooperación entre las administraciones aduaneras (DO C 24 de 23.1.1998, p. 1).

Disposiciones fundamentales

Los Estados miembros se asisten mutuamente para prevenir y detectar infracciones a las disposiciones aduaneras nacionales y perseguir y castigar infracciones a las disposiciones aduaneras nacionales y comunitarias. En el marco de investigaciones penales, el Convenio Nápoles II establece procedimientos con arreglo a los cuales las administraciones aduaneras pueden actuar conjuntamente e intercambiar datos, espontáneamente o previa petición, relativos a actividades de tráfico ilícito.

Las solicitudes se presentarán siempre por escrito, en una lengua oficial del Estado miembro al que pertenezca la autoridad requerida, o bien en otra aceptada por esta. Un formulario establece las normas para comunicar información. Las autoridades afectadas comunican toda la información que pueda ayudar a prevenir, detectar y perseguir infracciones. Intercambian datos personales, es decir, toda la información relativa a una persona física identificada o identificable.

En el marco de la asistencia que deba prestarse, la autoridad requerida, o la autoridad competente a la que haya recurrido esta última, procede como si actuase por su propia cuenta o a instancia de otra autoridad de su propio Estado miembro.

---

88 Decisión Marco 2002/475/JAI del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo (DO L 164 de 22.6.2002, p. 3).

89 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).

3.10.1. Sistema de Información Aduanero - SIA[90]

El Sistema de Información Aduanero complementa el Convenio de Nápoles II[91]. El sistema de información centralizado está gestionado por la Comisión y pretende mejorar la administración aduanera de los Estados miembros mediante un intercambio rápido de información para prevenir, investigar y perseguir violaciones graves de legislación comunitaria y nacional. El SIA también crea un fichero de identificación de los expedientes de investigaciones aduaneras (FIDE) para ayudar en las investigaciones aduaneras.

Las autoridades designadas por los Estados miembros[92] disponen de acceso directo a los datos contenidos en el SIA. Para mejorar la complementariedad con Europol y Eurojust, ambos organismos tendrán un acceso «solo lectura» al SIA y FIDE.

El SIA incluye datos personales con referencia a productos, medios de transporte, empresas, personas y mercancías, y efectivo retenidos, incautados o decomisados. Los datos personales solo pueden copiarse del SIA a otros sistemas de tratamiento de datos para gestión de riesgos o análisis operativo, a los que únicamente pueden acceder los analistas designados por los Estados miembros.

FIDE permite a las autoridades nacionales encargadas de llevar a cabo investigaciones aduaneras, cuando abren un expediente de investigación, identificar otras autoridades que pueden haber investigado a una persona o empresa determinada.

3.11. Organismos nacionales de recuperación de activos (ORA) y Red Interinstitucional de Recuperación de Activos de Camden (CARIN)

Legislación

Decisión 2007/845/JAI del Consejo, de 6 de diciembre de 2007, sobre cooperación entre los organismos de recuperación de activos de los Estados miembros en el ámbito del seguimiento y la identificación de productos del delito o de otros bienes relacionados con el delito (DO L 332 de 18.12.2007, p. 103).

La Red Interinstitucional de Recuperación de Activos de Camden (CARIN) fue creada en La Haya, los días 22 y 23 de septiembre de 2004, por Austria, Bélgica, Alemania, Irlanda, los Países Bajos y el Reino Unido.

---

90 Decisión 2009/917/JAI del Consejo, de 30 de noviembre de 2009, sobre la utilización de la tecnología de la información a efectos aduaneros (DO L 323 de 10.12.2009, p. 20).

91 Convenio relativo a la asistencia mutua y la cooperación entre las administraciones aduaneras, establecido sobre la base del artículo K.3 del Tratado de la Unión Europea (DO C 24 de 23.1.1998, p. 2).

92 Aplicación del artículo 7, apartado 2, y del artículo 8, apartado 3, de la Decisión 2009/917/JAI del Consejo, de 30 de noviembre de 2009, sobre la utilización de la tecnología de la información a efectos aduaneros - listas actualizadas de autoridades competentes (13394/11 ENFOCUSTOM 85).

Disposiciones fundamentales

A raíz de la adopción de la Decisión 2007/845/JAI del Consejo[93], todos los Estados miembros han establecido y designado organismos de recuperación de activos (ORA). Dichos organismos pueden intercambiar directamente información sobre cuestiones relativas a la recuperación de activos a través del sistema SIENA. Bajo los auspicios de la Comisión Europea y Europol, la red de ORA facilita la cooperación entre los organismos de recuperación de activos de los Estados miembros así como el debate estratégico y el intercambio de mejores prácticas. La Oficina de Activos de Origen Delictivo (ECAB) de Europol actúa como punto central para la recuperación de activos dentro de la UE.

Las disposiciones que establece la Directiva 2014/42/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, sobre el embargo y el decomiso de los instrumentos y del producto del delito en la Unión Europea[94] aumentarán la eficacia de la cooperación entre los organismos de recuperación de activos de la Unión Europea. Los Estados miembros tienen que transponer la Directiva antes del 4 de octubre de 2016.

La Red Interinstitucional de Recuperación de Activos de Camden (CARIN), creada en 2004 para apoyar la identificación, el embargo, la incautación y la confiscación transfronterizos de propiedades relacionados con delitos, intensifica el intercambio mutuo de información relativa a diferentes planteamientos nacionales con un alcance superior a la UE.

Desde 2015, la red CARIN engloba a profesionales de 53 jurisdicciones y 9 organizaciones internacionales que sirven de puntos de contacto a fin de agilizar el intercambio de información transfronterizo, previa petición o de manera espontánea. Los ORA nacionales cooperan entre sí, o con otras autoridades, a fin de facilitar el seguimiento y la identificación de productos del delito. Aunque todos los Estados miembros han establecido un ORA, existen grandes diferencias entre Estados miembros en términos de estructura organizativa, recursos y actividades.

---

93 Decisión 2007/845/JAI del Consejo, de 6 de diciembre de 2007, sobre cooperación entre los organismos de recuperación de activos de los Estados miembros en el ámbito del seguimiento y la identificación de productos del delito o de otros bienes relacionados con el delito (DO L 332 de 18.12.2007, p. 103).

94 Directiva 2014/42/UE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, sobre el embargo y el decomiso de los instrumentos y del producto del delito en la Unión Europea (DO L 127 de 29.4.2014, p. 39).

La información intercambiada puede utilizarse con arreglo a las disposiciones de protección de datos de los Estados miembros receptores y está sujeta a las mismas normas de protección de datos que si hubiera sido recogida en el Estado miembro receptor. Ha de fomentarse el intercambio espontáneo de información con arreglo a la presente Decisión, aplicando los procedimientos y plazos previstos en la denominada «Decisión Marco sueca».

3.12. Unidades de Información Financiera (UIF)

Legislación

Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión,
DO L 141 de 5.6.2015, p. 73.

Directiva (UE) 2019/1153 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otros tipos para la prevención, detección, investigación o enjuiciamiento de determinados delitos y por la que se deroga la Decisión 2000/642/JAI del Consejo,
DO L 186 de 11.7.2019, p. 122.

Disposiciones fundamentales

En virtud de lo dispuesto en la Directiva 2015/849 (la cuarta Directiva antiblanqueo, en su versión modificada por la Directiva 2018/843), cada Estado miembro debe constituir una UIF para prevenir, detectar y combatir eficazmente el blanqueo de capitales y la financiación del terrorismo. Como unidad nacional central, la UIF será responsable de recibir y analizar las comunicaciones de transacciones sospechosas y otra información relevante para el blanqueo potencial de capitales, los delitos subyacentes conexos o la potencial financiación del terrorismo. La UIF se encargará de comunicar a las autoridades competentes los resultados de sus análisis y cualquier información adicional relevante, cuando existan motivos para sospechar de la existencia de blanqueo de capitales, delitos subyacentes conexos o financiación del terrorismo. Estará en condiciones de obtener información adicional de las entidades obligadas. La UIF deberá estar en condiciones de responder a solicitudes de información de las autoridades competentes de sus respectivos Estados miembros cuando dichas solicitudes de información estén relacionadas con delitos subyacentes relacionados con el blanqueo de capitales o con posibles actividades de financiación del terrorismo.

Además del mencionado intercambio sobre blanqueo de capitales y financiación del terrorismo, la Directiva (UE) 2019/1153 establece que los Estados miembros velarán por que su UIF nacional también deba cooperar con las autoridades policiales designadas del Estado en cuestión y pueda responder a sus solicitudes motivadas de información financiera o de análisis financiero justificadas por cuestiones relativas a la prevención, detección, investigación o enjuiciamiento de infracciones penales graves, tal como se establece en el anexo 1 del Reglamento de Europol (2016/794).

En ambos casos, la UIF puede negarse a facilitar la información cuando existan razones objetivas para suponer que esta tendría un efecto negativo en las investigaciones en curso o cuando la divulgación de la información sea claramente desproporcionada respecto a los intereses legítimos de una persona física o jurídica, o irrelevante respecto a los fines para los que se haya solicitado.

De conformidad con lo dispuesto en la Directiva 2015/849 (la cuarta Directiva antiblanqueo) los Estados miembros deben garantizar que las UIF intercambien entre ellas, por propia iniciativa o previa solicitud, toda información que pueda ser pertinente para el tratamiento o el análisis por la UIF de información relacionada con el blanqueo de capitales o la financiación del terrorismo y sobre las personas físicas o jurídicas implicadas, con independencia del tipo de delitos subyacentes conexos e incluso si el tipo de delitos subyacentes conexos no ha sido identificado en el momento del intercambio. Una UIF podrá negarse a intercambiar información solo en circunstancias excepcionales en que el intercambio pudiera ser contrario a principios fundamentales del Derecho nacional. Los Estados miembros velarán por que la información intercambiada con arreglo a los artículos 52 y 53 se utilice únicamente para los fines para los que se haya solicitado o proporcionado.

Además del intercambio entre las UIF de distintos Estados miembros con arreglo a la Directiva 2015/849, la Directiva 2019/1153 establece ahora que, en casos urgentes y excepcionales, sus Unidades de Información Financiera estén autorizadas a intercambiar información financiera o análisis financieros que puedan ser pertinentes para el tratamiento o el análisis de información relacionada con el terrorismo o la delincuencia organizada relacionada con el terrorismo. La Directiva 2019/1153 también autoriza el intercambio de información entre las UIF y Europol.

La red de unidades de información financiera (FIU.NET) es una red informática descentralizada para el intercambio de información entre UIF.

La FIU.NET, que en principio estaba destinada a fortalecer la posición de las UIF, ha ido evolucionando en los últimos años y ha pasado de una herramienta básica segura para el intercambio bilateral de información a una herramienta multifuncional segura para el intercambio multilateral de información, con funciones de gestión de casos y una normalización de procesos semiautomatizada. En FIU.NET, cada nuevo dispositivo o proceso automatizado es optativo, sin consecuencias derivadas. Las UIF individuales pueden decidir qué posibilidades y dispositivos ofrecidos por FIU.NET utilizan; solo utilizan los dispositivos con los que trabajan a gusto y excluyen los que no necesiten o no deseen utilizar.

3.13. Acuerdo relativo al Programa de Seguimiento de la Financiación del Terrorismo (TFTP) entre la UE y los EE.UU.

Legislación

Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de seguimiento de la financiación del terrorismo,

DO L 195 de 27.7.2010, p. 5.

Disposiciones fundamentales

A raíz del 11S, la UE y los EE.UU. decidieron colaborar estrechamente y celebraron el Acuerdo sobre el tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo (Acuerdo TFTP UE -EE.UU.). De conformidad con el Acuerdo, el Departamento del Tesoro de los Estados Unidos también facilita información TFTP a la policía, la seguridad pública o las autoridades de la lucha antiterrorista de los Estados miembros de que se trate y, cuando proceda, a Europol y Eurojust.

El TFTP está dotado de fuertes medidas de control para garantizar el cumplimiento de los dispositivos de seguridad, incluidos los relativos a la protección de datos de carácter personal. Los datos se tratan exclusivamente con fines de prevención, investigación y enjuiciamiento del terrorismo o de su financiación. A los efectos del Acuerdo, el Departamento del Tesoro de los Estados Unidos podrá solicitar mensajería financiera sobre pagos y datos relacionados en el territorio de la UE procedente de los proveedores designados de servicios de mensajería financiera internacional sobre pagos.

Los beneficios que obtienen los Estados miembros, Europol y Eurojust de los datos TFTP se ven limitados por el hecho de que el análisis de los pagos transfronterizos TFTP se basa exclusivamente en mensajes FIN (mensajes de transferencias a instituciones financieras), un tipo de mensaje SWIFT mediante el cual la información financiera se transfiere de una institución financiera a otra. No se contempla ningún otro método de pago. Sin embargo, el TFTP es el único mecanismo que permite, en un periodo de tiempo muy breve, detectar y caracterizar las transacciones sospechosas de estar relacionadas con el terrorismo o con la financiación del terrorismo, a efectos de mejorar la seguridad interna. Debido a una mayor conciencia de las cláusulas de reciprocidad de este Acuerdo, las autoridades de la UE están aplicando cada vez más ese mecanismo con el fin de beneficiarse del intercambio de datos con los EE.UU. En este contexto, debe señalarse que todas las solicitudes de búsquedas en el TFTP procedentes de autoridades de la UE deben cumplir los requisitos contemplados en el artículo 10 del Acuerdo.

Aunque el Acuerdo no prevé que los Estados miembros soliciten a través de Europol una búsqueda de información pertinente obtenida a través del TFTP, sería conveniente que, con el fin de mejorar la respuesta de la UE al terrorismo y su financiación, los Estados miembros informaran al menos a Europol de manera sistemática y oportuna de sus solicitudes directas en virtud el artículo 10. Para ayudar a los Estados Miembros a canalizar sus solicitudes de búsqueda TFTP, Europol ha establecido un punto único de contacto (PUC), y gracias a su entorno de ficheros de análisis y a la cooperación establecida con el Tesoro, está en buenas condiciones para gestionar eficazmente las peticiones de los Estados miembros.

3.14. Intercambio de información de los registros de antecedentes penales (ECRIS)

Legislación

Decisión Marco 2009/315/JAI del Consejo, de 26 de febrero de 2009, relativa a la organización y al contenido del intercambio de información de los registros de antecedentes penales entre los Estados miembros (DO L 93 de 7.4.2009, p. 23). Esta Decisión Marco deroga la Decisión 2005/876/JAI del Consejo, de 21 de noviembre de 2005, relativa al intercambio de información de los registros de antecedentes penales (DO L 322 de 9.12.2005, p. 33).

Directiva (UE) 2019/884 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por la que se modifica la Decisión Marco 2009/315/JAI del Consejo en lo que respecta al intercambio de información sobre nacionales de terceros países y al Sistema Europeo de Información de Antecedentes Penales (ECRIS) y por la que se sustituye la Decisión 2009/316/JAI del Consejo (DO L 171 de 7.6.2019, p. 143).

Disposiciones fundamentales

La Decisión Marco 2009/315/JAI del Consejo exige a todo Estado miembro de condena que comunique cuanto antes al Estado miembro de nacionalidad de esa persona las condenas inscritas en sus registros de antecedentes penales, así como las eventuales modificaciones o cancelaciones posteriores de las mismas. El Estado miembro de nacionalidad tiene la obligación de conservar la información a efectos de retransmitirla. Cualquier modificación o cancelación de contenido realizada por el Estado miembro de condena entraña una modificación o cancelación idéntica en el registro de antecedentes penales del Estado miembro del que es nacional la persona. El Estado miembro del que es nacional la persona podrá solicitar información sobre condenas a efectos de un proceso penal o para cualquier otro fin que no sea un proceso penal, como la prevención de una amenaza inminente y grave para la seguridad pública. No obstante, la utilización de la información transmitida en virtud de la Decisión para fines distintos de un proceso penal puede limitarse con arreglo al Derecho nacional del Estado miembro requerido y del Estado miembro requirente, a fin de no poner en peligro las posibilidades de reinserción social de la persona condenada.

La Decisión 2009/316/JAI del Consejo determina la forma en la que el Estado miembro debe transmitir la información. La Decisión del Consejo establece el marco para un sistema informatizado de intercambio de la información extraída de los registros de antecedentes penales. Las autoridades centrales de cada Estado miembro utilizarán los formularios especiales de solicitud y respuesta anejos a la Decisión Marco, a través de la vía electrónica descrita en la legislación.

3.14.1. Intercambio de información sobre antecedentes penales de nacionales de terceros países y apátridas (ECRIS-TCN)

Legislación

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 (NTP) a fin de complementar y apoyar el Sistema Europeo de Información de Antecedentes Penales (ECRIS-TCN) y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 135 de 22.5.2019, p. 1).

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 de 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 modifica los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).

Directiva (UE) 2019/884 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, por la que se modifica la Decisión Marco 2009/315/JAI del Consejo en lo que respecta al intercambio de información sobre nacionales de terceros países y al Sistema Europeo de Información de Antecedentes Penales (ECRIS) y por la que se sustituye la Decisión 2009/316/JAI del Consejo (DO L 171 de 7.6.2019, p. 143).

Disposiciones fundamentales

El Reglamento se aplica al tratamiento de datos de identidad de aquellos nacionales de terceros países que hayan sido objeto de una condena en los Estados miembros. Por «nacional de un tercer país» se entiende una persona que no sea ciudadano de la Unión en el sentido del artículo 20, apartado 1, del TFUE, o una persona que sea apátrida o de nacionalidad desconocida. Los antecedentes penales relativos a estas personas se conservan en el Estado miembro donde se pronunció la condena. El objetivo del ECRIS-TCN[95] es determinar qué otros Estados miembros poseen dicha información sobre antecedentes penales. Después puede utilizarse el marco del ECRIS para solicitar dicha información a los Estados miembros en cuestión, de conformidad con la Decisión Marco 2009/315/JAI.

El Reglamento contiene disposiciones por las que se establece un sistema que contiene datos personales, desarrollados y mantenidos por la eu-LISA y centralizados a nivel de la Unión, y disposiciones sobre el reparto de responsabilidades entre el Estado miembro y la organización responsable del desarrollo y mantenimiento del sistema centralizado. Establece un grado general adecuado de protección de los datos, seguridad de los datos y protección de los derechos fundamentales de las personas afectadas.

[95] La Comisión determinará la fecha a partir de la cual deberá comenzar a funcionar el ECRIS-TCN, una vez que se cumplan las condiciones establecidas en el artículo 35 del Reglamento (UE) 2019/816.

Eurojust, Europol y la Fiscalía Europea, deben tener acceso al ECRIS-TCN para identificar a los Estados miembros que posean información sobre antecedentes penales de un nacional de un tercer país, con el fin de poder desempeñar las funciones que le han sido encomendadas.

3.15. Conservación de datos de las telecomunicaciones

Legislación

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE[96].

Disposiciones fundamentales

La Directiva se aplica a los proveedores de servicios de comunicaciones electrónicas. La Directiva establece que los proveedores deben conservar los datos de tráfico y de localización, así como los datos relacionados necesarios para identificar al abonado o usuario, con el fin de comunicar esos datos a las autoridades nacionales competentes que lo soliciten. Con fines de investigación, detección y enjuiciamiento de delitos graves, los Estados miembros obligan a los proveedores de servicios de comunicaciones electrónicas o de redes públicas de comunicaciones a conservar las categorías de datos necesarios para identificar:

- el origen de una comunicación;
- el destino de una comunicación;
- la fecha, hora y duración de una comunicación
- el tipo de comunicación;
- el equipo de comunicación de los usuarios o lo que se considere su equipo de comunicación;
- la localización del equipo de comunicación móvil.

No podrá conservarse ningún dato que revele el contenido de la comunicación.

[96] La sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014 declaró inválida la Directiva.

3.16. Directiva PNR (registro de nombres de los pasajeros)

Legislación

Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

Disposiciones fundamentales

La Directiva establece a escala de la Unión un marco legal común para la transferencia y tratamiento de datos PNR y dispone:

b) la transferencia por parte de las compañías aéreas[97] de los datos del registro de nombres de los pasajeros (PNR) de vuelos exteriores de la UE. En caso de que un Estado miembro decida aplicar la Directiva a los vuelos interiores de la UE, todas las disposiciones se aplicarán a los vuelos interiores de la UE como si se tratara de vuelos exteriores de la UE.

c) El tratamiento de los datos PNR, incluida su recogida, utilización y conservación por los Estados miembros, así como el intercambio de los mismos entre dichos Estados miembros.

A efectos del tratamiento de los datos PNR, cada Estado miembro establece o designa una autoridad competente para actuar como su Unidad de Información sobre los Pasajeros (UIP). Dos o más Estados miembros podrán establecer o designar una autoridad única que actúe como una UIP común.

Los datos PNR que figuran en el anexo I de la Directiva han de transferirse a la UIP en la medida en que las compañías aéreas ya los hayan recopilado en el transcurso normal de su actividad. Algunas compañías aéreas conservan los datos de información anticipada sobre los pasajeros (API) como parte de los datos PNR, mientras que otras no. Con independencia de la manera en que las compañías áreas recopilan la API, dichas compañías la transferirán a las UIP, para que estas la traten de la misma manera que los datos PNR. En el anexo II de la Directiva figura la lista de los «delitos graves» en el ámbito de aplicación de la Directiva.

---

97 La Directiva no afecta a la posibilidad de que los Estados miembros establezcan en su derecho nacional un mecanismo para recoger y tratar los datos PNR proporcionados por operadores económicos que no sean compañías aéreas, tales como agencias de viaje y operadores turísticos que prestan servicios relacionados con los viajes, como la reserva de vuelos, para los cuales recogen y tratan datos PNR, o de los transportistas que no sean los mencionados en él, siempre que el derecho nacional de que se trate respete el derecho de la Unión.

El tratamiento de los datos PNR sirve para la evaluación de los pasajeros antes de su llegada o salida del Estado miembro a fin de identificar a las personas que deban ser examinadas de nuevo por las autoridades competentes a efectos de prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y la delincuencia grave, y, cuando proceda, por Europol dentro de los límites de sus competencias y para el desempeño de sus funciones.

Para efectuar la evaluación, las UIP pueden:

a) comparar los datos PNR con las bases de datos pertinentes a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, incluidas las bases de datos sobre personas u objetos buscados o bajo alerta, de acuerdo con las normas de la Unión, internacionales y nacionales aplicables a dichas bases de datos, o

b) tratar los datos PNR con arreglo a criterios predeterminados.

A escala nacional, las UIP transmiten los datos PNR o el resultado de su tratamiento a los servicios de seguridad nacionales competentes habilitados para examinar de nuevo el expediente o tomar las medidas adecuadas para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves. Aunque las UIP constituyen el canal de intercambio de información transfronteriza principal, las autoridades competentes pueden dirigirse directamente a las UIP desde otro Estados miembro en caso de emergencia y bajo condiciones bien definidas.

A escala de la Unión, las IUP intercambian los datos PNR y el resultado del tratamiento de dichos datos entre sí y con Europol, que estará habilitado, dentro de los límites de sus competencias y para el desempeño de sus funciones, para solicitar dichos datos de las UIP.

Los datos PNR se conservarán en una base de datos de la UIP durante un plazo de cinco años a partir de su transmisión desde el Estado de llegada o de salida del vuelo. No obstante, todos los datos PNR deberán despersonalizarse tras un periodo de seis meses. Esto se llevará a cabo enmascarando todos aquellos elementos que pudieran servir para identificar directamente al pasajero al que se refieren dichos datos. La lista de los datos PMR que han de enmascararse figura en la Directiva. Después de transcurridos cinco años, los datos PNR deberán suprimirse a menos que hayan sido transferidos a una autoridad competente a efectos de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, en cuyo caso, será la legislación nacional la que regule su conservación.

De conformidad con la legislación de la UE sobre protección de datos, la Directiva PNR prohíbe el tratamiento de datos sensibles relacionados con la raza o el origen étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato, la salud o la vida u orientación sexual de la persona.

3.17. Información anticipada sobre los pasajeros (datos API)

Legislación

Directiva 2004/82/CE del Consejo de 29 de abril de 2004 sobre la obligación de los transportistas de comunicar los datos de las personas transportadas,

Disposiciones fundamentales

El objetivo de la Directiva es mejorar los controles fronterizos y combatir la inmigración ilegal. A este efecto, la Directiva exige a los Estados miembros que impongan a las compañías aéreas la obligación de comunicar determinada información sobre sus viajeros antes de entrar en la Unión Europea. Dicha información se conoce como Información anticipada sobre los pasajeros (datos API). Bajo determinadas condiciones y circunstancias, los Estados miembros también pueden utilizar los datos API a efectos policiales.

La información es proporcionada a petición de las autoridades responsables de efectuar los controles de personas en las fronteras exteriores de la UE.

Las compañías aéreas transmitirán los datos API por medios electrónicos, o, si ello no fuera posible, por cualquier otro medio adecuado, a las autoridades encargadas de realizar los controles fronterizos al entrar el pasajero en la UE. Los datos API se cotejarán con las bases de datos nacionales y europeas, como el Sistema de Información de Schengen (SIS) y el Sistema de Información de Visados (VIS).

Cuando los datos API coincidan con una entrada en una base de datos, se envía una descripción a la policía de fronteras y el pasajero correspondiente es seleccionado para su examen a la llegada.

Los datos API recogidos y transmitidos deberán ser suprimidos pos los transportistas y las autoridades en el plazo de veinticuatro horas de su transmisión o de la llegada. No obstante, las autoridades fronterizas podrán conservar los ficheros temporalmente más de veinticuatro horas si los datos fueran a ser necesarios posteriormente a efectos de ejercer las funciones estatutarias de las autoridades fronterizas o para aplicar la legislación y las normativas relativas a la entrada y la inmigración, en particular las disposiciones sobre protección del orden público y de la seguridad nacional.

3.18. Infracciones de tráfico en materia de seguridad vial

Legislación

Directiva (UE) 2015/413 del Parlamento Europeo y del Consejo, de 11 de marzo de 2015, por la que se facilita el intercambio transfronterizo de información sobre infracciones de tráfico en materia de seguridad vial (DO L 68 de 13.3.2015, p. 9).

Disposiciones fundamentales

Los Estados miembros se conceden recíprocamente acceso en red a sus datos de matriculación de vehículos (DMV), con el fin de aplicar las sanciones impuestas por infracciones de tráfico en materia de seguridad vial cometidas con un vehículo matriculado en un Estado miembro distinto del Estado miembro en el que se cometió la infracción. El Estado miembro de la infracción utiliza los datos obtenidos con el fin de determinar quién es la persona responsable de la infracción de tráfico. El intercambio de información se refiere a:

- el exceso de velocidad;
- la no utilización del cinturón de seguridad;
- no respetar un semáforo en rojo;
- la conducción en estado de embriaguez;
- la conducción bajo los efectos de drogas;
- la no utilización del casco de protección;
- la circulación por un carril prohibido;
- utilización ilegal de un teléfono móvil o de cualquier otro dispositivo de comunicación durante la conducción.

Mediante la aplicación informática específica EUCARIS, los Estados miembros conceden a sus puntos de contacto nacionales acceso recíproco a sus DMV, con posibilidad de efectuar búsquedas automatizadas de

a) datos relativos a los vehículos y

b) datos relativos al propietario o titular del vehículo.

3.19. Sistema de Entradas y Salidas (SES)

Legislación

Reglamento (UE) 2017/2226 del Parlamento Europeo y del 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 (DO L 327 de 9.12.2017, p. 20).

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 de 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 modifica los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).

El Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen.

Dinamarca ha notificado que ha decidido aplicar los citados Reglamentos en virtud del artículo 4 del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea. Esta decisión crea una obligación, en virtud del Derecho internacional, entre Dinamarca y los demás Estados miembros vinculados por las medidas.

El Reino Unido e Irlanda no participan en el acervo y, por lo tanto, no están vinculados por el Reglamento ni sujetos a su aplicación.

Islandia, Noruega, Liechtenstein y Suiza están vinculados al acervo en el sentido de los respectivos acuerdos o protocolos relativos al acervo de Schengen.

Por lo que se refiere a Chipre, Bulgaria, Rumanía y Croacia, las disposiciones del Reglamento relativas al SIS y al VIS constituyen disposiciones que desarrollan el acervo de Schengen o están relacionadas con él de otro modo en el sentido de las respectivas Actas de Adhesión.

Disposiciones fundamentales

El Reglamento[98] especifica los objetivos del SES, las categorías de datos que se introducirán en el sistema, los fines para los que se utilizarán, los criterios de introducción, las autoridades facultadas para acceder a los datos, otras normas en materia de tratamiento de datos y protección de datos personales, así como la arquitectura técnica del SES, las normas relativas a su funcionamiento y utilización, y la interoperabilidad con otros sistemas de información. El objeto del SES es mejorar la gestión de las fronteras exteriores, prevenir la inmigración irregular y facilitar la gestión de los flujos migratorios. Con este fin, el SES está concebido para registrar y almacenar la fecha, la hora y el lugar de entrada y salida de los nacionales de terceros países que cruzan las fronteras de aquellos Estados miembros en los que se utilice el SES. Además, las autoridades policiales nacionales pueden consultar el SES a efectos de prevención, detección o investigación de delitos de terrorismo y otros delitos graves[99].

El SES consiste en un sistema central (sistema central del SES), que gestiona una base central informatizada de datos biométricos y alfanuméricos, y una interfaz nacional uniforme en cada Estado miembro. Un canal de comunicación seguro conecta el sistema central del SES con el Sistema Central de Información de Visados (sistema central del VIS), y una infraestructura de comunicaciones segura y cifrada conecta el sistema central del SES con la interfaz nacional uniforme. La interoperabilidad entre el SES y el VIS se establece a través de un canal de comunicación directa entre los sistemas centrales de estos, a fin de que las autoridades fronterizas puedan consultar el VIS desde el SES y las autoridades responsables de los visados consultar el SES desde el VIS.

---

98 La Comisión determinará la fecha a partir de la cual deberá comenzar a funcionar el SES, una vez que se cumplan las condiciones establecidas en el artículo 66 del Reglamento (UE) 2017/2226.

99 Por «delito de terrorismo» se entiende un delito que coincida o sea equivalente a alguno de los delitos recogidos en la Directiva (UE) 2017/541; Por «delito grave» se entiende el delito que corresponda o sea equivalente a alguno de los delitos recogidos en el artículo 2, apartado 2, de la Decisión Marco 2002/584/JAI relativa a la orden de detención europea, que esté castigado en el Derecho nacional con una pena privativa de libertad o de internamiento de una duración máxima no inferior a tres años.

El Reglamento establece normas estrictas sobre el acceso al EES. Asimismo, establece los derechos de acceso, rectificación, compleción, supresión y compensación de las personas, en particular el derecho de recurso judicial y la supervisión de las operaciones de tratamiento por autoridades públicas independientes.

El Reglamento respeta los derechos fundamentales y observa los principios reconocidos por la Carta de los Derechos Fundamentales de la UE. Sin perjuicio de las normas más específicas establecidas en el Reglamento para el tratamiento de datos personales, el Reglamento (UE) n.º 2016/679[100] («Reglamento General de Protección de datos») se aplica al tratamiento de datos personales en aplicación de dicho Reglamento, a menos que el tratamiento sea realizado por las autoridades policiales designadas o los puntos de acceso central de los Estados miembros, en los que se aplica la Directiva 2016/680/UE[101] («Directiva sobre policía»).

3.20. Sistema Europeo de Información y Autorización de Viajes (SEIAV)

Legislación

Reglamento (UE) 2018/1240 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se crea 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).

Reglamento (UE) 2018/1241 del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se modifica el Reglamento (UE) 2016/794 con objeto de establecer el Sistema Europeo de Información y Autorización de Viajes (SEIAV), DO L 236 de 19.9.2018, p. 72.

---

100 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).

101 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2019 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),

El Reglamento 2018/1240[102] especifica los objetivos del SEIAV, define su arquitectura y organización técnica, establece normas relativas al funcionamiento y el uso de los datos que el solicitante debe introducir en el sistema y normas sobre la expedición o denegación de las autorizaciones de viaje, establece los fines para los que pueden tratarse los datos, determina las autoridades autorizadas a acceder a los datos y garantiza la protección de los datos personales.

El Reglamento constituye un desarrollo de las disposiciones del acervo de Schengen. El Reino Unido e Irlanda no participan en el acervo y, por lo tanto, no están vinculados por el Reglamento ni sujetos a su aplicación. Islandia, Noruega, Liechtenstein y Suiza están vinculados al acervo en el sentido de los respectivos acuerdos o protocolos relativos al acervo de Schengen.

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 de 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 modifica los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).

Disposiciones fundamentales

El SEIAV establece una autorización de viaje que es, por naturaleza, independiente de un visado, pero constituye una condición de entrada y residencia en la zona Schengen, e indica que el solicitante de la autorización de viaje no supone una amenaza para la seguridad, un riesgo de inmigración ilegal ni un peligro elevado de epidemia para la Unión.

El SEIAV está compuesto por

- un sistema de información a gran escala, esto es, el sistema de información SEIAV, diseñado, desarrollado y gestionado técnicamente por la eu-LISA;

[102] La Comisión determinará la fecha a partir de la cual deberá comenzar a funcionar el SEIAV, una vez que se cumplan las condiciones establecidas en el artículo 88 del Reglamento (UE) 2018/1240.

- la unidad central del SEIAV, que forma parte de la Agencia Europea de la Guardia de Fronteras y Costas;

- las unidades nacionales SEIAV, encargadas de examinar las solicitudes y de decidir expedir o rechazar, anular o retirar las autorizaciones de viaje. Con este fin, han de cooperar entre ellas y con Europol para evaluar las solicitudes.

El acceso a los datos personales del SEIAV ha de quedar limitado al personal estrictamente autorizado y en ningún caso debe utilizarse para adoptar decisiones basadas en alguna forma de discriminación. Por lo que respecta a las autoridades policiales designadas por los Estados miembros, el tratamiento de los datos almacenados en el sistema central del SEIAV solo debe producirse en casos concretos y solo cuando sea necesario a efectos de prevención, detección o investigación de delitos de terrorismo o delitos graves. Las autoridades designadas y Europol solo deben solicitar acceso al SEIAV cuando tengan motivos fundados para pensar que dicho acceso facilitará información que les ayude en la prevención, detección o investigación de un delito de terrorismo o un delito grave.

El Reglamento respeta los derechos fundamentales y cumple los principios reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea. Por lo que respecta al tratamiento de los datos personales, hay, por lo tanto, salvaguardas apropiadas cuyo objeto es limitar la interferencia con el derecho a la protección de la vida privada y el derecho a la protección de los datos personales a lo que estrictamente necesario y proporcionado en una sociedad democrática.

El Reglamento para el tratamiento de datos personales, el Reglamento (UE) n.º 2016/679[103] («Reglamento General de Protección de datos») se aplica al tratamiento de datos personales en aplicación de dicho Reglamento, a menos que el tratamiento sea realizado por las autoridades policiales designadas o los puntos de acceso central de los Estados miembros, en los que se aplica la Directiva 2016/680/UE[104] («Directiva sobre policía»).

---

103 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 (DO L 119 de 4.5.2016, p. 1).

104 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2019 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).

3.21. Legislación sobre interoperabilidad

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 de 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 modifica los Reglamentos (UE) 2018/1726, (UE) 2018/1862 y (UE) 2019/816 (DO L 135 de 22.5.2019, p. 85).

Disposiciones fundamentales

El Reglamento (UE) 2019/817 y el Reglamento (UE) 2019/818 constituyen el «paquete de interoperabilidad» y se centran en los datos personales almacenados en sistemas de información centralizados a nivel de la UE. Su objeto es mejorar la arquitectura de gestión de datos de la Unión en lo que respecta tanto a la gestión de las fronteras como a la seguridad. Así pues, el marco del «paquete de interoperabilidad» se aplica al tratamiento de datos personales en el ámbito de las fronteras y los visados, la cooperación policial y judicial, el asilo y la migración. La interoperabilidad entre estos sistemas de información subyacente ha de permitirles complementarse mutuamente para cumplir sus objetivos respectivos.

Los Reglamentos también adaptan los procedimientos y las condiciones para el acceso de las autoridades designadas y de Europol al SES, al VIS, al SEIAV y a Eurodac con fines de prevención, detección o investigación de delitos de terrorismo y delitos graves.

Los componentes técnicos de la interoperabilidad abarcan el SES (véase el punto 3.18), el VIS (véase el punto 3.7), el SEIAV (véase el punto 3.19), Eurodac (véase el punto 3.8), el SIS (véase el punto 3.2) y el sistema ECRIS-TCN (véase el punto 3.13.2). Los componentes de la interoperabilidad[105] son los siguientes:

- el portal europeo de búsqueda, entendido como una ventanilla única o un «intermediario de mensajes», que permite consultar los instrumentos de la UE, los datos de Europol y las bases de datos de Interpol en paralelo. Las consultas se limitan a los datos relativos a personas o documentos de viaje;

[105] La Comisión determinará la fecha a partir de la cual deberán comenzar a aplicarse las disposiciones de los Reglamentos relacionadas con el PEB, el SCB compartido, el RCDI y el DIM.

- El servicio de correspondencia biométrica (SCB) compartido, cuyo objetivo principal es facilitar la identificación de una persona registrada en varias bases de datos, utilizando un único componente tecnológico para cotejar los datos biométricos de dicha persona entre diferentes sistemas. Las plantillas de SAID en uso deben reagruparse y almacenarse en un único lugar en el Sistema de Correspondencias Biométricas;

- el registro común de datos de identidad (RCDI), entendido como un repositorio común de los datos de identidad, documentos de viaje y datos biométricos de las personas registradas en el SES, el VIS, el SEIAV, Eurodac y el ECRIS-TCN. Dichos datos pueden referirse a la misma persona, pero con identidades distintas o incompletas. Mediante una comparación automatizada y el cotejo de los datos debe conseguirse una mayor precisión de la identificación. El RCDI establece controles de identidad por parte de las autoridades policiales designadas para ayudarles en su labor de identificación de una persona;

- un detector de identidades múltiples (DIM), que contribuye al funcionamiento del RCDI.

Las nuevas operaciones de tratamiento de datos previstas por los Reglamentos interfieren con los derechos fundamentales protegidos por los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la UE. 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 en consonancia con los 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.

El Reglamento (UE) 2016/679 se aplica al tratamiento de datos personales con fines de interoperabilidad, a menos que sean las autoridades policiales 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 delitos de terrorismo o delitos graves. En ese caso se aplica la Directiva (UE)2016/680 (véase el punto 3.0).

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.