BASE DE DATOS DE Norma CEF.-
Referencia: NCL012628

LEY ORGÁNICA 1/2020, de 16 de septiembre, sobre la utilización de los datos del Registro de Nombres de Pasajeros para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.

(BOE de 17 de septiembre de 2020)

FELIPE VI
REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente

LEY ORGÁNICA

PREÁMBULO

I

La protección de la vida y de la seguridad de los ciudadanos constituye el objetivo principal del espacio de libertad, seguridad y justicia de la Unión Europea. Entre las medidas que se han adoptado para su consecución, el Consejo de la Unión Europea, a través del «Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano», de 4 de mayo de 2010, instó a la Comisión a presentar una propuesta sobre la utilización de datos del Registro de Nombres de los Pasajeros («Passenger Name Record», en adelante PNR) para prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves.

Asimismo, en el plano internacional se ha venido avanzando en la dimensión exterior de esta política de la Unión Europea. La Comisión presentó una serie de elementos esenciales de la misma en su Comunicación de 21 de septiembre de 2010 «Sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países», y la Unión alcanzó diversos acuerdos internacionales con distintos Estados.

El incremento de la amenaza del crimen organizado y especialmente del terrorismo en Europa constituyen violaciones muy graves de los valores universales de la dignidad humana, la libertad, la igualdad, la solidaridad y el disfrute de los derechos humanos y de la libertades fundamentales en los que se basa la Unión Europea. Con el objetivo de elevar los niveles de seguridad de sus ciudadanos y de crear un marco jurídico para la protección de sus datos de carácter personal, en lo que respecta a su tratamiento por las autoridades competentes, se adoptó la 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.

Con este fin se insta a los Estados miembros a que introduzcan en sus ordenamientos internos las disposiciones legales pertinentes para que los datos PNR de los vuelos exteriores de la Unión Europea sean transferidos a una Unidad de Información sobre Pasajeros que se cree en cada Estado, sin perjuicio de que pueda también aplicarse a los vuelos interiores de la Unión, según el criterio de cada país, como prevé la aludida Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, posibilidad de la que se hace uso en esta ley orgánica.

Asimismo, la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, exige la creación de un sistema uniforme en la Unión Europea para el tratamiento de los datos PNR, precisando claramente cuáles son estos, los fines a los que se limita su recogida, la utilización y transmisión, el establecimiento de unidades únicas de información sobre los pasajeros en cada Estado miembro, así como la obligatoriedad de la adopción de medidas que faciliten el cumplimiento por los operadores de sus deberes, incluida la imposición de sanciones efectivas, proporcionadas y disuasorias ante eventuales incumplimientos.

El tratamiento de los datos PNR va a mejorar la respuesta a la amenaza del terrorismo y la delincuencia grave mediante el cotejo de tales datos con las bases de datos disponibles y pertinentes, a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, y el análisis y

evaluación de los mismos utilizando unos criterios específicos y revisables periódicamente, que permitan la identificación de personas que pudieran estar relacionadas con este tipo de actividades criminales, al tiempo que minimizarán al máximo el riesgo de afectar a personas inocentes.

II

Esta ley orgánica se estructura en tres capítulos, treinta y cuatro artículos, seis disposiciones adicionales y cuatro disposiciones finales.

El capítulo I establece las disposiciones generales.

Su objeto es regular, por un lado la transferencia de los datos PNR por parte de las compañías aéreas y otras entidades obligadas; en segundo término, la recogida, el tratamiento y la protección de esos datos, su transmisión a las autoridades competentes y el intercambio de dichos datos con otros Estados miembros, Europol y terceros Estados; a su vez, la designación de la Unidad de Información sobre Pasajeros española, y por último, el régimen sancionador.

Se especifican los fines para los que pueden ser utilizados los datos PNR, únicamente para prevenir, detectar, investigar y enjuiciar delitos de terrorismo y delitos graves.

El ámbito de aplicación contempla, en principio, todos los vuelos internacionales que tengan origen, destino o tránsito en España, tanto de carácter comercial como privados, con una serie de excepciones basadas en el tipo de los vuelos.

Excepcionalmente, como medida extraordinaria y siempre que existan indicios suficientes de una contrastada situación de riesgo, se podrán sujetar rutas o vuelos concretos de ámbito nacional a lo dispuesto en esta ley orgánica.

Asimismo, se definen los sujetos obligados, diferenciando las compañías áreas de las entidades de gestión de reservas de vuelos, cuya incorporación en esta ley orgánica es una posibilidad prevista en Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Se determinan también los delitos de terrorismo y los demás delitos graves cuya prevención, detección, investigación o enjuiciamiento justifica la recogida de los datos PNR. Los delitos de terrorismo son los contemplados en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, como delitos de las organizaciones y grupos terroristas y delitos de terrorismo. En cuanto a los demás delitos graves, se considera como tales, a los efectos de esta ley, aquellos castigados con una pena de prisión igual o superior a tres años por ser constitutivos de algunos de los enumerados en el anexo II de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Por otro lado, se especifican los datos de los pasajeros que deben ser enviados a la Unidad de Información sobre Pasajeros, de entre los recopilados por parte de los sujetos obligados para sus propios fines comerciales en el transcurso normal de su actividad. Entre estos figuran los datos contenidos en el sistema de información anticipada sobre pasajeros (sistema API), algunos de los cuales, a diferencia de los anteriores, han sido contrastados con los documentos oficiales de identificación.

Deberá enviarse también cierta información sobre la tripulación correspondiente a los datos API. Asimismo, en el caso de los vuelos privados se deberán enviar dichos datos tanto de los pasajeros como de los tripulantes. Es imprescindible, para la consecución de las finalidades previstas en la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, disponer de tales datos de tripulaciones y de vuelos privados, sin los cuales se podrían correr graves riesgos de seguridad pública, como ha demostrado la experiencia de los últimos años.

El capítulo II se ocupa del tratamiento de los datos PNR.

Se regula la Unidad de Información sobre Pasajeros española (UIP), incardinada en la estructura del Centro de Inteligencia contra el Terrorismo y el Crimen Organizado dependiente de la Secretaría de Estado de Seguridad, órgano con experiencia en materia de coordinación y en la recepción y análisis de la información estratégica disponible en la lucha contra todo tipo de terrorismo y delincuencia organizada.

Se determinan sus funciones, referidas tanto a la recepción, tratamiento y análisis de los datos PNR, como a las comunicaciones e intercambios de estos con las autoridades competentes nacionales y unidades análogas de otros Estados miembros, terceros países y Europol.

Se regula específicamente la figura del responsable de protección de datos, cuyo principal cometido será el de garantizar la rigurosa observancia de la legislación vigente en materia de protección de datos de carácter personal durante todo el proceso de recepción, tratamiento, transmisión, conservación y supresión de los datos PNR.

La transmisión de datos se llevará a cabo utilizando los formatos determinados y los protocolos definidos en la Decisión de Ejecución de la Comisión UE 2017/759, 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.

Las compañías aéreas informarán a la UIP del formato y protocolo de transmisión que utilizarán. Con respecto a las compañías aéreas que no dispongan de la infraestructura técnica necesaria, se contempla la posibilidad de acordar con el Ministerio del Interior los medios electrónicos de transmisión, siempre que se respeten las garantías de seguridad.

Los datos serán enviados en dos momentos distintos; el primero entre las cuarenta y ocho y las veinticuatro horas anteriores a la salida programada del vuelo, y el segundo se producirá una vez cerrado el vuelo, es decir, en el momento a partir del cual nadie puede entrar en el avión ni abandonarlo. Si durante el vuelo se produce alguna modificación en el destino, también deberá ser transmitida.

Cuando sea necesario acceder a los datos PNR para responder a una amenaza real y concreta en momentos distintos a los anteriores, caso por caso, las compañías aéreas deberán transmitir a la UIP dichos datos con carácter inmediato al requerimiento recibido.

Sin perjuicio de las obligaciones establecidas en esta ley orgánica, los tratamientos de datos de carácter personal realizados por los sujetos obligados se regirán por lo dispuesto en el 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 la legislación interna que se dicte en uso de la habilitación contenida en aquel.

En relación con el tratamiento de los datos de carácter personal por parte de las autoridades competentes, estas estarán sujetas al deber de proporcionar o poner a disposición del interesado la información y facilitar el ejercicio de los derechos de estos contemplados en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la ley orgánica que la incorpore a nuestro ordenamiento interno.

En este capítulo también se definen los propósitos para los que la UIP realizará el tratamiento de los datos PNR mediante la utilización de una definida metodología: Evaluar a las personas a bordo de la aeronave a fin de identificar a aquellas que pudieran tener relación con delitos de terrorismo o delitos graves; revisar individualmente los resultados de dicha evaluación previa automatizada; responder peticiones de las autoridades competentes o de Europol y establecer criterios predeterminados a utilizar en esas evaluaciones.

Para ello, la UIP cotejará los datos PNR con las bases de datos disponibles y pertinentes a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, y tratará los datos de acuerdo con los criterios predeterminados. Se realizará una verificación automática a priori, que, en el caso de ofrecer un resultado positivo, requerirá necesariamente una comprobación manual por parte de un especialista de la propia UIP.

Se precisa cuáles son las autoridades competentes que pueden solicitar o recibir datos PNR o el resultado del tratamiento de dichos datos por la UIP, con el objetivo de seguir examinando dicha información o adoptar las medidas adecuadas para prevenir, detectar, investigar y enjuiciar delitos de terrorismo y delitos graves. Estas son las Direcciones Generales de la Policía y de la Guardia Civil, el Centro Nacional de Inteligencia, la Dirección Adjunta de Vigilancia Aduanera y el Ministerio Fiscal. También se contemplan como autoridades competentes las correspondientes de las Comunidades Autónomas que hayan asumido estatutariamente competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana y cuenten con un cuerpo de policía propio. Los Jueces y Tribunales, en garantía del principio de independencia constitucional, se regirán en cuanto a las peticiones de dicha información y a la colaboración con la UIP por lo dispuesto en su legislación específica.

Las peticiones de las autoridades competentes serán debidamente motivadas y con suficiente base. En ningún caso se admitirán peticiones masivas y no fundamentadas. Todo tratamiento que lleven a cabo estas autoridades competentes sobre los datos recibidos de la UIP, lo será para los fines propios de la lucha contra los delitos de terrorismo y los delitos graves.

El capítulo recoge, además, una serie de disposiciones en materia de protección de datos, entre las que figuran la obligación de conservación de la documentación relativa a los sistemas y procedimientos de tratamiento; la obligación de registro de las operaciones de recogida, consulta, transferencia y supresión de los datos, así como la obligación de comunicar al interesado y a la autoridad nacional de control cualquier violación de los datos personales que dé lugar a un elevado riesgo para la protección de los mismos o afecte negativamente a la intimidad del interesado.

En una Europa concebida como espacio de libertad, seguridad y justicia, la colaboración y cooperación entre los Estados miembros cobra una especial relevancia. Y dentro de esa cooperación, los aspectos relativos a la seguridad se han tornado fundamentales en los últimos años en la lucha contra el terrorismo y la criminalidad organizada. En esa línea de colaboración, España podrá enviar datos PNR o el resultado de su tratamiento a otros Estados miembros, de oficio o atendiendo una solicitud concreta. Las peticiones entre Estados han de ser motivadas y siempre orientadas al cumplimiento de los fines previstos en esta ley orgánica.

Se contempla la posibilidad de que una autoridad competente española pueda dirigirse directamente a la Unidad de Información sobre Pasajeros de otro Estado miembro para una solicitud de información, siempre que se den conjuntamente las circunstancias de urgencia e imposibilidad de comunicación con la UIP nacional. En todo caso se remitirá copia de la petición a la UIP española.

La transferencia de datos a Europol se llevará a cabo electrónicamente y de forma motivada, siempre que entre dentro del ámbito de sus competencias y sea necesaria para el ejercicio de sus funciones.

Se incluye el procedimiento de transmisión de datos a terceros países. En este intercambio se tendrá que observar lo establecido en la legislación que transponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Además, deberá tratarse de una transmisión de datos necesaria para los fines de esta ley orgánica, y el Estado receptor de los mismos solamente podrá transmitirlos, a su vez, a otro tercer Estado si cuenta para ello con la expresa autorización de la Unidad española. En todo caso, se garantizará que la transmisión y la utilización de datos PNR a terceros Estados mantengan unos estándares y garantías como los previstos en esta ley orgánica.

En garantía del derecho a la intimidad de los sujetos afectados y en especial de su derecho a la protección de datos de carácter personal, se contempla que los datos PNR facilitados a la UIP por los sujetos obligados serán conservados durante cinco años a contar desde su transmisión. Una vez transcurridos seis meses desde su recepción, los datos PNR que permitan la identificación directa del pasajero serán despersonalizados mediante enmascaramiento, y solo se permitirá el acceso a la totalidad de los mismos previa aprobación por la autoridad judicial o por la persona titular de la Secretaría de Estado de Seguridad.

Cumplido el plazo de los cinco años serán suprimidos definitivamente, sin perjuicio de su utilización por parte de las autoridades competentes que los hayan recibido y que los estén utilizando en el marco de un asunto concreto a efectos de prevenir, detectar, investigar o enjuiciar delitos de terrorismo o delitos graves.

Por último, se regulan en este capítulo las competencias de la Agencia Española de Protección de Datos en su condición de autoridad nacional de control de datos PNR.

El capítulo III, que regula el régimen sancionador, se limita a establecer las especialidades estrictamente necesarias por razón de la materia, aplicándose en lo demás el régimen general previsto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Así, se definen los sujetos responsables, los regímenes especiales de responsabilidad y el concurso de normas; se tipifican las infracciones que se clasifican en muy graves, graves y leves; se determinan las sanciones según la infracción de que se trate, para cuya graduación se tendrá en cuenta la repercusión en la seguridad pública, la gravedad, o el beneficio obtenido, entre otras circunstancias; se determina la competencia sancionadora; y, finalmente, se incluyen las normas procedimentales especiales sobre los gastos derivados de la adopción de posibles medidas provisionales por parte del órgano competente para resolver, así como sobre la caducidad del procedimiento.

En las disposiciones adicionales se regula el plazo en el que las compañías aéreas deberán comunicar a la UIP el formato de datos y el protocolo de transmisión que utilizarán; se establece que las comunicaciones se harán según los procedimientos establecidos por la Secretaría de Estado de Seguridad; y se establecen normas referentes a la transmisión de los datos PNR remitidos a determinadas autoridades competentes como son el Centro Nacional de Inteligencia, las Direcciones Generales de la Policía y de la Guardia Civil, la Dirección Adjunta de Vigilancia Aduanera y los Jueces y Tribunales y el Ministerio Fiscal.

Además, contiene cuatro disposiciones finales, relativas al título competencial, a los preceptos que tienen carácter de ley orgánica, a la incorporación de derecho de la Unión Europea y a la entrada en vigor.

III

En la elaboración de esta ley orgánica se han observado los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia, de acuerdo con el artículo 129 de la Ley 39/2015, de 1 de octubre. Se trata de una norma necesaria para la transposición de la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, cuya aprobación goza de las garantías correspondientes al rango de ley orgánica por suponer un desarrollo de derechos fundamentales de los ciudadanos.

Por último, está incluida en el Plan Anual Normativo para 2018 aprobado por el Consejo de Ministros en su reunión de 7 de diciembre de 2017.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Esta ley orgánica, con el propósito de garantizar y proteger la vida y la seguridad de los ciudadanos, tiene por objeto regular:

a) La transferencia de datos del registro de nombres de los pasajeros (en adelante datos PNR), así como de la información de la tripulación referida en el artículo 5.3, correspondientes a vuelos internacionales y, en su caso, nacionales, en los términos y a los efectos previstos en el capítulo II.

b) El sistema de recogida, uso, almacenamiento, tratamiento, protección, acceso y conservación de los datos PNR, la transmisión de dichos datos a las autoridades competentes, así como el intercambio de los mismos con los Estados miembros de la Unión Europea, con Europol y con terceros países.

c) La determinación y atribución de las funciones de la Unidad de Información sobre Pasajeros española.

d) El régimen sancionador aplicable a las infracciones de conformidad con lo dispuesto en esta ley orgánica.

2. Los datos PNR podrán ser objeto de tratamiento únicamente con la finalidad de prevenir, detectar, investigar y enjuiciar los delitos de terrorismo y los delitos graves que se enumeran en el artículo 4, y de acuerdo con los propósitos establecidos en el artículo 12.2.

Artículo 2. *Ámbito de aplicación.*

1. Esta ley orgánica será de aplicación, en todo caso, a los datos PNR correspondientes a las personas que viajen en los vuelos internacionales, tanto interiores como exteriores de la Unión Europea, con su salida del territorio español o llegada al mismo, o que hagan escala en él. En este último supuesto, siempre se entenderán comprendidos los pasajeros en tránsito o en conexión, con las precisiones establecidas en el apartado siguiente.

2. Su ámbito de aplicación se extiende a los vuelos comerciales y a los vuelos privados.

No será de aplicación a los vuelos realizados por aeronaves de Estado y por aeronaves privadas, fletadas por el Estado para la prestación o apoyo de servicios de interés militar y en general servicios estatales no comerciales, durante los vuelos dedicados exclusivamente a materializar tal prestación o apoyo, que se asimilarán a las aeronaves de Estado, a los trabajos aéreos, a la aviación general que no tenga por objeto el transporte de personas, a los servicios aeroportuarios, a los servicios de navegación aérea, a los vuelos relacionados con la producción de aeronaves civiles, a los vuelos de entrenamiento de tripulaciones, a los vuelos de traslado para mantenimiento y revisión y a los vuelos relacionados con funciones regulatorias.

3. Como medida extraordinaria y por el tiempo que resulte imprescindible, será de aplicación a las rutas o a los vuelos concretos nacionales, que no efectúen escalas en ningún otro Estado, siempre que existan indicios suficientes de una clara y contrastada situación de riesgo, con la finalidad de prevenir, detectar, investigar y enjuiciar los delitos a los que se refiere el artículo 4.

La determinación de tales rutas o vuelos será acordada por el Consejo de Ministros, a propuesta del titular del Ministerio del Interior, teniendo en cuenta el carácter extraordinario de la medida, su necesidad y proporcionalidad.

Artículo 3. *Sujetos obligados.*

1. Son sujetos obligados las compañías aéreas, entendiendo como tales las empresas de transporte aéreo con una licencia de explotación válida o similar para el transporte por vía aérea.

A los efectos de esta ley orgánica, la definición de empresa será la establecida en el Reglamento (CE) 1008/2008 del Parlamento Europeo y del Consejo, de 24 de septiembre de 2008, sobre normas comunes para la explotación de servicios aéreos en la Comunidad, comprendiendo cualquier persona física o jurídica, con o sin fines de lucro, o cualquier organismo oficial dotado o no de personalidad jurídica propia.

En el caso de los vuelos privados serán sujetos obligados los operadores de las aeronaves bien sea como propietarios, arrendatarios o en virtud de otro título posesorio reconocido por la legislación vigente.

2. Son igualmente sujetos obligados las entidades de gestión de reserva de vuelos, entendiendo como tales a las entidades que gestionen reservas de vuelos de pasajeros y recaben datos PNR de los mismos, cualesquiera que sean los medios utilizados para ello, tales como los operadores turísticos o las agencias de viajes, que estarán obligadas en los términos previstos en el artículo 9.2.

Artículo 4. *Delitos de terrorismo y delitos graves.*

1. A los exclusivos efectos de esta ley orgánica, son delitos de terrorismo los contemplados en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, como delitos de las organizaciones y grupos terroristas y delitos de terrorismo.

2. Asimismo, a los exclusivos efectos de esta ley orgánica, son delitos graves aquellos que la ley castigue con una pena de prisión igual o superior a tres años por ser constitutivos de:

a) Pertenencia a una organización delictiva.
b) Trata de seres humanos.
c) Explotación sexual de niños y pornografía infantil.
d) Tráfico ilícito de estupefacientes y sustancias psicotrópicas.
e) Tráfico ilícito de armas, municiones y explosivos.
f) Corrupción.
g) Fraude, incluido el que afecte a los intereses financieros de la Unión Europea.
h) Blanqueo del producto del delito y falsificación de moneda, con inclusión del euro.
i) Delitos informáticos/ciberdelincuencia.
j) Delitos contra el medio ambiente, incluido el tráfico ilícito de especies animales protegidas y de especies y variedades vegetales protegidas.
k) Ayuda a la entrada y residencia ilegales.
l) Homicidio voluntario, agresión con lesiones graves.
m) Tráfico ilícito de órganos y tejidos humanos.
n) Secuestro, detención ilegal y toma de rehenes.
ñ) Robo organizado y a mano armada.
o) Tráfico ilícito de bienes culturales, incluidas las antigüedades y las obras de arte.
p) Falsificación y violación de derechos de propiedad intelectual o industrial de mercancías.
q) Falsificación de documentos administrativos y tráfico de documentos administrativos falsos.
r) Tráfico ilícito de sustancias hormonales y otros factores de crecimiento.
s) Tráfico ilícito de materiales radiactivos o sustancias nucleares.
t) Violación.
u) Delitos incluidos en la jurisdicción de la Corte Penal Internacional.
v) Secuestro de aeronaves y buques.
w) Sabotaje.
x) Tráfico de vehículos robados.

y) Espionaje industrial.

Artículo 5. *Datos del Registro de Nombres de Pasajeros (datos PNR).*

1. Los datos PNR son el conjunto de datos relativos al viaje de un pasajero, reservado por él o en su nombre, que recoge la información necesaria para la gestión de la reserva.

2. Los datos PNR relativos a los pasajeros son los siguientes:

a) Localizador de registro PNR.
b) Fecha de reserva y de emisión del billete.
c) Fechas previstas del viaje.
d) Nombres y apellidos.
e) Dirección y datos de contacto (número de teléfono, dirección de correo electrónico).
f) Todos los datos de pago, incluida la dirección de facturación.
g) Itinerario completo del viaje para el PNR específico.
h) Información sobre viajeros frecuentes.
i) Agencia de viajes u operador de viajes.
j) Situación de vuelo del pasajero: confirmaciones, facturación, no comparecencia o pasajeros de última hora sin reserva.
k) Información PNR escindida o dividida.
l) Observaciones generales, incluida toda la información disponible sobre menores de dieciocho años no acompañados, como nombre, apellidos, y sexo del menor, edad, idiomas que habla, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de salida y vínculo con el menor, nombre, apellidos y dirección de contacto del acompañante en el aeropuerto de llegada y vínculo con el menor, agente en el lugar de salida y de llegada.
m) Información sobre el billete, incluidos el número del billete, la fecha de emisión, los billetes solo de ida y la indicación de la tarifa de los billetes electrónicos (Automatic Ticket Fare Quote).
n) Datos del asiento, incluido el número.
ñ) Información sobre códigos compartidos.
o) Toda la información relativa al equipaje.
p) Número de viajeros y otros nombres de viajeros que figuran en el PNR.
q) Cualquier información recogida en el sistema de información anticipada sobre los pasajeros (sistema API), incluidos el tipo, número, país de emisión y fecha de expiración de cualquier documento de identidad, nacionalidad, apellidos, nombre, sexo, fecha de nacimiento, compañía aérea, número de vuelo, fecha de salida, fecha de llegada, aeropuerto de salida, aeropuerto de llegada, hora de salida y hora de llegada.
r) Todo el historial de cambios de los datos PNR indicados en los párrafos a) a q).

3. En el caso de los vuelos comerciales las disposiciones de esta ley orgánica serán aplicables, además de a los datos de los pasajeros, a los datos de la tripulación en el caso del párrafo q) y a los datos de cualquier otra persona a bordo señalados en los párrafos o) y q) del apartado anterior. Igualmente, en el caso de los vuelos privados, serán de aplicación a tales datos de los pasajeros y tripulantes.

CAPÍTULO II

Tratamiento de los datos PNR

Artículo 6. *Unidad de Información sobre Pasajeros.*

1. La Unidad de Información sobre Pasajeros española (UIP) se integra orgánicamente en el Centro de Inteligencia contra el Terrorismo y el Crimen Organizado, dependiente de la Secretaría de Estado de Seguridad del Ministerio del Interior.

2. La UIP es la responsable del tratamiento de los datos PNR.

Artículo 7. *Funciones y facultades.*

1. La UIP realizará exclusivamente las siguientes funciones:

a) Recoger los datos PNR, almacenarlos, tratarlos y transferir, en su caso, dichos datos o el resultado de su tratamiento a las autoridades competentes.
b) Intercambiar tanto los datos PNR como el resultado de su tratamiento con las Unidades de Información sobre Pasajeros de otros Estados miembros de la Unión Europea, con Europol y con terceros países.

2. Para la realización de las funciones mencionadas en el apartado anterior, la UIP será responsable de:

a) Analizar, relacionar y valorar los datos obtenidos.
b) Establecer y actualizar criterios útiles para identificar a las personas que puedan estar implicadas en delitos de terrorismo y delitos graves, en cooperación, en su caso, con las autoridades competentes.
c) Elaborar informes de inteligencia estratégica y de análisis de riesgo.
d) Colaborar con las autoridades competentes encargadas de las investigaciones y actuaciones operativas, así como elaborar los protocolos de actuación pertinentes en colaboración con las mismas.
e) Poner los hechos que puedan ser constitutivos de las infracciones previstas en esta ley orgánica en conocimiento del órgano competente para sancionarlas.
f) Elaborar estadísticas anuales sobre su actividad, incluyendo el número total de personas cuyos datos PNR hayan sido recopilados e intercambiados, así como el número de personas identificadas para un examen ulterior.

3. El almacenamiento, tratamiento y análisis de los datos PNR se llevará a cabo exclusivamente en uno o varios lugares seguros dentro del territorio nacional.

4. Cuando fuere preciso para el desarrollo de sus funciones, el personal al servicio de las autoridades competentes enumeradas en el artículo 14 podrá prestar servicios en la UIP. Dicho personal continuará en servicio activo en su Cuerpo dependiendo orgánica, funcional y retributivamente de su Administración de origen, sin perjuicio de que en el desarrollo de sus funciones en la UIP haya de atenerse a lo preceptuado para la misma respecto a su organización y funcionamiento.

Artículo 8. *Responsable de protección de datos.*

1. La UIP designará una persona como responsable de protección de los datos PNR que velará por que se adopten las medidas oportunas para controlar el tratamiento de estos datos y por que se apliquen las garantías en materia de protección de datos. El responsable de protección de datos actuará como punto de contacto único, al que cualquier interesado tendrá derecho a dirigirse para todas las cuestiones relativas al tratamiento de sus datos PNR.

2. La persona designada lo será atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados de la legislación y las prácticas en materia de protección de datos personales, y a su capacidad para desempeñar las funciones contempladas en esta ley orgánica. Deberá contar con los medios necesarios para el desempeño de sus funciones de manera eficaz e independiente.

3. La persona responsable de la protección de datos tendrá acceso a todos los datos PNR tratados por la UIP. Si considerase que el tratamiento de un dato no ha sido lícito, lo pondrá en conocimiento del responsable del tratamiento para que se adopten las medidas correctoras necesarias y, si lo estima oportuno, podrá remitir el asunto a la autoridad nacional de control.

4. En lo no previsto en esta ley orgánica se regirá por lo regulado para los delegados de protección de datos en la legislación que transponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se

deroga la Decisión Marco 2008/977/JAI del Consejo, y hasta ese momento por las normas que regulen en Derecho español el tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

Artículo 9. *Obligaciones de transmisión de datos.*

1. Las compañías aéreas enviarán los datos PNR correspondientes a los vuelos comprendidos en el artículo 2 que hayan recopilado en el transcurso normal de su actividad, a la base de datos de la UIP. En el caso de los vuelos privados, el operador asumirá la responsabilidad de que la información prevista en el artículo 5.3 sea remitida a la UIP.

En el caso de que existan varias compañías aéreas relacionadas con un mismo vuelo, la obligación de transmitir los datos recaerá en la compañía aérea que actúe como operadora del mismo.

2. Las entidades de gestión de reservas de vuelos introducirán en el PNR los datos que hayan recopilado en el transcurso normal de su actividad respecto a los vuelos comprendidos en el artículo 2.

3. En el cumplimiento de sus obligaciones de información, y sin perjuicio de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y en la legislación interna que se dicte en uso de la habilitación contenida en aquel, los sujetos obligados informarán a las personas a las que se refieran los datos PNR del motivo de su recogida y de su destinatario, la Unidad de Información sobre Pasajeros, ante cuyo responsable de protección de datos podrán dirigirse para todas las cuestiones relativas al tratamiento de sus datos PNR.

4. Las compañías aéreas enviarán los datos PNR a la UIP, utilizando en todo caso medios electrónicos que ofrezcan garantías suficientes en relación con las medidas de seguridad técnicas y las medidas organizativas que rigen el tratamiento de datos que se va a llevar a cabo. Esta transmisión se realizará con arreglo a uno de los formatos de datos y mediante uno de los protocolos de transmisión establecidos en la Decisión de Ejecución de la Comisión (UE) 2017/759, 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.

En el caso de que transmitan datos API sobre los pasajeros de manera separada respecto del resto de los datos PNR para el mismo vuelo, deberán utilizar, para su envío a la UIP, el formato específico de datos que contempla la Decisión de Ejecución de la Comisión (UE) 2017/759, de 28 de abril de 2017.

En caso de fallo técnico o imposibilidad sobrevenida, realizarán la transmisión de los datos PNR, en el plazo más breve posible, por cualquier otro medio apropiado que garantice un nivel adecuado de seguridad de dichos datos.

5. Las compañías aéreas que no operen vuelos con arreglo a un calendario concreto y público y que no dispongan de la infraestructura técnica necesaria para usar los formatos de datos y los protocolos de transmisión incluidos en la Decisión de Ejecución de la Comisión (UE) 2017/759, de 28 de abril de 2017, utilizarán, para la transmisión de los datos PNR, los formatos y los medios electrónicos que se acuerden de forma bilateral entre la compañía aérea y el Ministerio del Interior, siempre que ofrezcan garantías suficientes respecto de las medidas de seguridad técnicas. Este régimen será el aplicable en todo caso a los vuelos privados.

Artículo 10. *Momentos de la transmisión de datos.*

1. Los momentos en los que las compañías aéreas deben transmitir los datos PNR a la UIP serán los siguientes:

a) Entre las veinticuatro y las cuarenta y ocho horas antes de la hora de salida programada del vuelo, e

b) inmediatamente después del cierre del vuelo, una vez que los pasajeros hayan embarcado en el avión en preparación de la salida y no sea posible embarcar o desembarcar.

Las compañías aéreas podrán limitar esta transmisión prevista en el párrafo b) a las actualizaciones de la información transmitida conforme al párrafo a).

2. Las compañías aéreas deberán comunicar cualquier cambio producido previamente o durante el trayecto, respecto al destino donde se tuviera previsto aterrizar o a la realización de una escala no programada.

3. Además, cuando sea necesario acceder a los datos PNR para responder a una amenaza real y concreta relacionada con delitos de terrorismo o con delitos graves, en momentos distintos de los previstos en el apartado 1, todos los sujetos obligados, caso por caso, deberán transmitir a la UIP dichos datos con carácter inmediato al requerimiento recibido.

Artículo 11. *Régimen jurídico aplicable al tratamiento de datos PNR.*

1. Los tratamientos de datos de carácter personal que lleven a cabo la UIP y las autoridades competentes referidas en el artículo 14 se regirán por esta ley orgánica y supletoriamente por la legislación que transponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y hasta ese momento por las normas que regulen en Derecho español el tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales. En este régimen jurídico se incluye la protección de los datos personales de los pasajeros y sus derechos de acceso, rectificación, supresión, limitación del tratamiento, indemnización y recurso judicial.

2. Sin perjuicio de las obligaciones establecidas en esta ley orgánica, los tratamientos de datos de carácter personal realizados por los sujetos obligados referidos en el artículo 3 se regirán por lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y por la legislación interna que se dicte en uso de la habilitación contenida en aquel.

Artículo 12. *Tratamiento de los datos PNR.*

1. Los datos PNR serán recogidos por la UIP.

Si la información transmitida incluyera datos distintos de los relacionados en esta ley orgánica, la UIP los suprimirá inmediatamente y de manera definitiva en el momento de su recepción.

2. La UIP tratará los datos PNR solo para los siguientes propósitos:

a) Realizar una evaluación de los pasajeros y de la tripulación antes de la llegada o salida programada del vuelo, a fin de identificar a las personas que deban ser examinadas de nuevo por las autoridades competentes y, en su caso, por Europol ante la posibilidad de que pudieran estar implicadas en un delito de terrorismo o en un delito grave.

b) Responder en cada caso particular a las peticiones de las autoridades competentes, debidamente motivadas y con suficiente base, para que les transfieran datos PNR en supuestos específicos a efectos de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, así como el resultado de su tratamiento.

c) Analizar los datos PNR con el fin de establecer o actualizar criterios que deben utilizarse en las evaluaciones realizadas en virtud del apartado 3.b), con el objeto de identificar a las personas que puedan estar implicadas en delitos de terrorismo o delitos graves.

Estos criterios de evaluación predeterminados deberán ser proporcionados y específicos y estar orientados a la finalidad que persiguen. No se basarán en el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato o partido político, la salud o la vida u orientación sexual de la persona. La UIP establecerá y revisará periódicamente estos criterios, en colaboración con las autoridades competentes.

3. Al realizar la evaluación a que se refiere el apartado 2.a), la UIP podrá someter los datos PNR a las siguientes operaciones:

a) Comparará los datos PNR con todas las bases de datos disponibles y pertinentes, a los efectos de la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves.
b) Tratará los datos PNR de acuerdo con los criterios predeterminados establecidos para identificar a las personas que puedan estar implicadas en delitos de terrorismo o en delitos graves.

4. Cuando la evaluación efectuada de acuerdo con el apartado 2.a) arrojara un resultado positivo, la UIP procederá a la revisión individual de tal resultado a través de medios no automatizados, con el fin de comprobar la necesidad de que las autoridades competentes realicen un examen ulterior o emprendan las acciones o inicien los procedimientos oportunos. A tal fin, la UIP deberá transmitir los datos PNR a las autoridades competentes.

Artículo 13. *Consecuencias de la evaluación.*

Las consecuencias de las evaluaciones de los pasajeros a las que se refiere el apartado 2.a) del artículo anterior, no perjudicarán el derecho de entrada en España de las personas que gocen del derecho de libre circulación en la Unión Europea.
Cuando estas evaluaciones se efectúen en relación con pasajeros de vuelos interiores de la Unión Europea a los que sea aplicable el Reglamento (UE) 2016/399 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, por el que se establece un Código de normas de la Unión para el cruce de personas por las fronteras, las consecuencias se ajustarán a lo previsto en dicho reglamento.

Artículo 14. *Autoridades competentes.*

1. Las autoridades competentes para solicitar o recibir de la UIP datos PNR o el resultado del tratamiento de dichos datos a fin de seguir examinando esa información o de adoptar las medidas adecuadas para prevenir, detectar, investigar y enjuiciar delitos de terrorismo y delitos graves, serán las siguientes:

a) La Dirección General de la Policía.
b) La Dirección General de la Guardia Civil.
c) El Centro Nacional de Inteligencia.
d) La Dirección Adjunta de Vigilancia Aduanera.
e) El Ministerio Fiscal.
f) Las correspondientes de las Comunidades Autónomas que hayan asumido estatutariamente competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana, y cuenten con un cuerpo de policía propio.

2. Las peticiones de datos realizadas por las autoridades competentes serán debidamente motivadas y con suficiente base. En ningún caso se admitirán peticiones masivas y no fundamentadas.

3. Las autoridades competentes colaborarán con la UIP, en el ámbito de sus competencias, para el cumplimiento de los fines de esta ley orgánica.

4. A los Jueces y Tribunales, que tendrán la consideración de autoridades competentes, no les serán de aplicación los apartados 2 y 3, en atención al principio constitucional de independencia del poder judicial, rigiéndose en cuanto a las peticiones de datos y a la colaboración con la UIP por lo que establezca la legislación aplicable al ejercicio de la función jurisdiccional.

5. Los datos remitidos por la UIP a las autoridades competentes podrán ser objeto de tratamiento posterior por estas, únicamente con los fines específicos de prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, sin perjuicio de las acciones o procedimientos que puedan realizarse o iniciarse en el caso de que, como consecuencia del tratamiento de dichos datos, se detecten otros delitos o indicios de ellos.

6. Las autoridades competentes no adoptarán ninguna decisión que produzca efectos jurídicos adversos para una persona o que afecte negativamente a una persona únicamente en razón del tratamiento automatizado de datos PNR.

Dichas decisiones no deberán basarse en el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato o partido político, la salud o la vida y orientación sexual de la persona.

Artículo 15. *Protección de los datos de carácter personal.*

1. La UIP no podrá tratar datos PNR que revelen el origen racial o étnico, las opiniones políticas, las creencias religiosas o filosóficas, la pertenencia a un sindicato o partido político, la salud, la vida o la orientación sexual de la persona. En el caso de que reciba datos PNR que revelen tal información, los suprimirá inmediatamente.

2. La UIP conservará la documentación relativa a todos los sistemas y procedimientos de tratamiento bajo su responsabilidad.

Dicha documentación constará como mínimo de los siguientes elementos:

a) Los datos identificativos del personal de la UIP encargado del tratamiento de los datos PNR, así como del responsable de protección de datos, y los distintos niveles de autorización de acceso;

b) las solicitudes cursadas por las autoridades competentes y por las Unidades de Información sobre Pasajeros de otros Estados miembros y;

c) todas las solicitudes y transmisiones de datos PNR a un tercer país o a Europol.

La UIP pondrá esta documentación a disposición de la autoridad nacional de control a petición de esta, de acuerdo con la legislación vigente.

3. La UIP llevará registros, al menos, de las operaciones de recogida, consulta, transferencia y supresión de los datos.

Los registros de consulta y transferencia mostrarán, en particular, la finalidad, la fecha y la hora de tales operaciones y, en la medida de lo posible, la identidad de la persona que consultó o transmitió los datos PNR y la identidad de los receptores de dichos datos.

Los registros se utilizarán exclusivamente a efectos de verificación, autocontrol, y garantía de la integridad de los datos y de su seguridad o de auditoría. Dichos registros se conservarán por un período de cinco años.

La UIP pondrá los registros a disposición de la autoridad nacional de control a petición de esta, de acuerdo con la legislación aplicable.

4. Cuando sea probable que una violación de los datos personales dé lugar a un elevado riesgo para la protección de estos o afecte negativamente a la intimidad del interesado, la UIP comunicará, sin demora injustificada, dicha violación al interesado y a la autoridad nacional de control.

5. La UIP aplicará las medidas y los procedimientos técnicos y organizativos adecuados para garantizar un elevado nivel de seguridad correspondiente a los riesgos que entrañen el tratamiento y las características de los datos PNR.

Artículo 16. *Intercambio de información entre Estados miembros de la Unión Europea.*

1. La UIP transmitirá los datos PNR pertinentes y necesarios o el resultado de su tratamiento, relativos a las personas identificadas por la misma como personas que puedan estar implicadas en un delito de terrorismo o en un delito grave, a las Unidades de Información sobre Pasajeros de los otros Estados miembros. Dicha transmisión sólo se llevará a cabo tras un análisis de cada caso y, en supuestos de tratamiento automatizado de los datos PNR, tras una revisión individualizada por medios no automatizados.

En caso de que la UIP reciba datos PNR o el resultado de su tratamiento de la Unidad de Información sobre Pasajeros de otro Estado miembro deberá proporcionar todos los datos pertinentes y necesarios, a las autoridades competentes correspondientes, tras una revisión individualizada.

2. La UIP tendrá derecho a solicitar, en cada caso concreto, para la prevención, detección, investigación o enjuiciamiento de delitos de terrorismo o delitos graves, a la Unidad de Información sobre Pasajeros de cualquier otro Estado miembro, que le suministre los datos PNR almacenados en su base de datos y que no hayan sido despersonalizados mediante enmascaramiento de elementos de los datos, así como, si fuera necesario, el resultado de cualquier tratamiento de los mismos. La solicitud deberá ser debidamente motivada.

En el caso de que hayan sido despersonalizados mediante enmascaramiento de elementos de datos, la transmisión tendrá lugar de conformidad con el derecho nacional aplicable en el Estado miembro de la Unidad de Información sobre Pasajeros requerida.

3. A su vez, la Unidad de Información sobre Pasajeros de cualquier Estado miembro podrá solicitar directamente a la UIP datos PNR o el resultado de su tratamiento, bajo las mismas condiciones previstas en el apartado anterior. En ese caso, la UIP proporcionará la información solicitada lo antes posible.

En el supuesto de que los datos requeridos hayan sido despersonalizados mediante enmascaramiento, la UIP únicamente proporcionará los datos completos o el resultado de su tratamiento ante casos específicos cuando sea necesario para la prevención, detección, investigación y enjuiciamiento de delitos de terrorismo y delitos graves, y sólo cuando lo haya autorizado la autoridad judicial o la persona titular de la Secretaría de Estado de Seguridad.

4. Las autoridades competentes que requieran datos PNR recabados por un Estado miembro de la Unión Europea canalizarán sus solicitudes de forma motivada a través de la UIP.

Únicamente cuando no sea posible dirigir sus peticiones a través de la UIP y en caso de urgencia, y siempre que la solicitud cumpla con las condiciones establecidas en el apartado 2, las autoridades competentes podrán solicitar dichos datos directamente a la Unidad de Información sobre Pasajeros de otro Estado miembro.

De estas solicitudes directas y urgentes se remitirá copia a la UIP, al mismo tiempo que a la Unidad de Información sobre Pasajeros del Estado miembro de que se trate, que deberá acompañarse, lo antes posible, de una motivación de la remisión directa.

5. De manera excepcional, cuando sea necesario acceder a los datos PNR para responder a una amenaza concreta y real relacionada con delitos de terrorismo o delitos graves, la UIP solicitará a la Unidad de Información sobre Pasajeros del Estado miembro correspondiente que acceda a los datos PNR fuera de los momentos ordinarios de transmisión establecidos en el artículo 10 y que se los transmita.

Del mismo modo, la UIP responderá lo antes posible a las solicitudes que reciba de otros Estados miembros en los supuestos previstos en el párrafo anterior.

6. El intercambio de información previsto en este artículo podrá realizarse utilizando cualquiera de las vías existentes de cooperación entre las autoridades competentes de los Estados miembros.

Artículo 17. *Transferencia de datos a Europol.*

1. La UIP transferirá los datos PNR específicos o el resultado de su tratamiento solicitados por Europol, caso por caso, de forma electrónica y debidamente motivada, cuando sea estrictamente necesario para apoyar y reforzar la acción de un Estado miembro de la Unión Europea a efectos de prevenir, detectar, investigar o enjuiciar delitos de terrorismo o delitos graves, siempre que el delito entre dentro del ámbito de competencias de Europol y para el desempeño de sus funciones.

2. La solicitud indicará las causas razonables por las que Europol considera que la transmisión de los datos PNR o de los resultados de su tratamiento va a contribuir significativamente a prevenir, detectar o investigar la infracción penal en cuestión.

3. Europol informará al responsable de la protección de datos de cada uno de los intercambios de información en virtud de este artículo.

4. El intercambio de información se realizará a través de la Red de Intercambio Seguro de Información (SIENA).

Artículo 18. *Transferencias de datos a terceros países no miembros de la Unión Europea.*

1. La UIP podrá transferir a terceros países no miembros de la UE datos PNR, así como el resultado de su tratamiento, en casos concretos y si se cumplen concurrentemente los siguientes requisitos:

a) Las condiciones establecidas para las transferencias de datos a terceros países en la legislación que transponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y hasta ese momento por las normas que regulen en Derecho español el tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales.
b) La transmisión resulta necesaria para los fines señalados en el artículo 1.2.
c) El tercer país se compromete a transmitir los datos PNR a otro tercer país sólo si fuera estrictamente necesario para los fines de esta ley orgánica y siempre contando con la autorización expresa de la UIP.
d) Los previstos en el artículo 16.

2. Las transmisiones de datos PNR por la UIP sin consentimiento previo del Estado miembro del que fueron obtenidos se permitirán en circunstancias excepcionales y únicamente si:

a) Son esenciales para responder a una amenaza específica y real relacionada con delitos de terrorismo o delitos graves de un Estado miembro o de un tercer país y;
b) el consentimiento previo no pudo obtenerse a su debido tiempo.

La UIP informará sin demora a la autoridad del Estado miembro responsable de dar el consentimiento. La transmisión se registrará por la UIP y podrá ser objeto de una verificación posterior.

3. Cada vez que la UIP transfiera datos PNR a terceros países en virtud de lo previsto en este artículo, su responsable de protección de datos será informado.

4. La UIP exclusivamente transmitirá datos PNR a las autoridades competentes de terceros países tras asegurarse de que se ajustan a un estándar de condiciones y garantías equivalente al de esta ley orgánica y de que la utilización de los datos PNR prevista por los receptores se ajusta a dichas condiciones y garantías.

Artículo 19. *Período de conservación de los datos y despersonalización.*

1. Los datos PNR proporcionados a la UIP por los sujetos obligados se conservarán en una base de datos de la Unidad durante un plazo de cinco años a partir de la fecha de su transmisión a la UIP.

2. Transcurrido un plazo de seis meses desde la transmisión a la que se refiere el apartado 1, todos los datos PNR deberán ser despersonalizados mediante enmascaramiento, de manera que resulten invisibles para un usuario los siguientes elementos que servirían para identificar directamente a los afectados:

a) Nombres y apellidos, incluidos los de otros pasajeros que figuran en el PNR, y número de personas que figuran en el PNR que viajan juntas;
b) dirección y datos de contacto;
c) todos los datos sobre el pago, incluida la dirección de facturación, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el registro PNR, o a cualquier otra persona;
d) información sobre viajeros frecuentes;
e) observaciones generales, en la medida en que contengan información que pueda servir para identificar directamente al pasajero al que se refiere el registro, y
f) todos los datos API sobre los pasajeros.

3. Al finalizar el período de seis meses mencionado en el apartado 2, solo se permitirá la transmisión de los datos completos cuando concurran las dos circunstancias siguientes:

a) Que sea necesario a los efectos establecidos en el artículo 12.2.b).

b) Que haya sido aprobada por una autoridad judicial o por la persona titular de la Secretaría de Estado de Seguridad. En este último caso, se informará de la transmisión al responsable de protección de datos de la UIP, y estará sujeta a la revisión, a posteriori, por parte del mismo.

4. Los datos PNR serán suprimidos de modo permanente al finalizar el período a que se refiere el apartado 1. Esta obligación se entenderá sin perjuicio de aquellos casos en que se hayan transferido datos PNR específicos a una autoridad competente y esta los esté utilizando en el marco de un asunto concreto a efectos de prevenir, detectar, investigar o enjuiciar delitos de terrorismo o delitos graves, en cuyo caso la conservación de los datos por la autoridad competente se regirá por la normativa específica.

5. Los resultados del tratamiento a que se refiere el artículo 12.2.a) serán conservados por la UIP durante el tiempo necesario para informar de un resultado positivo a las autoridades competentes y a las Unidades de Información sobre Pasajeros de otros Estados miembros.

Cuando el resultado de un tratamiento automatizado, tras un examen individual por medios no automatizados, arroje un resultado negativo, se podrá almacenar para evitar falsos resultados positivos posteriores, mientras los datos de base no se hayan eliminado según el apartado 4.

Artículo 20. *Competencias de la Agencia Española de Protección de Datos.*

Además de las competencias que le otorga su normativa específica, la Agencia Española de Protección de Datos, en su condición de autoridad nacional de control de datos PNR a los efectos previstos en esta ley orgánica, ejercerá las siguientes competencias:

a) Asesorar, previa solicitud, sobre la aplicación de las disposiciones adoptadas en España para aplicar la Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y controlar su aplicación con el fin de proteger los derechos fundamentales de cualquier interesado en lo relativo al tratamiento de datos personales.

b) Conocer de las reclamaciones presentadas contra los tratamientos realizados al amparo de esta ley orgánica y dar respuesta a las mismas en un plazo de tiempo razonable.

c) Verificar la legalidad de los tratamientos, por propia iniciativa o como consecuencia de una reclamación, para lo cual podrá realizar investigaciones, inspecciones y auditorías, de acuerdo con lo dispuesto en su normativa reguladora, sin perjuicio de las funciones que corresponden al Consejo General del Poder Judicial como autoridad de control de los tratamientos de datos vinculados al ejercicio de la función jurisdiccional.

CAPÍTULO III

Régimen sancionador

SECCIÓN 1.ª DISPOSICIONES GENERALES

Artículo 21. *Sujetos responsables.*

La responsabilidad por las infracciones cometidas recaerá directamente en los sujetos obligados que, por acción u omisión, realizaran la conducta en que consista la infracción.

Artículo 22. *Responsable de tratamiento y responsable de protección de datos.*

La responsabilidad del responsable de tratamiento de los datos PNR y del responsable de protección de datos PNR se determinará de acuerdo con lo dispuesto en la legislación que transponga la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y hasta ese momento por las normas que regulen en Derecho español el tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección y enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

Artículo 23. *Regla especial.*

A los efectos exclusivos de esta ley orgánica, se entenderá que los incumplimientos de la obligación de transmisión o remisión de los datos PNR que se produzcan en relación a un mismo vuelo constituyen una única infracción.

Artículo 24. *Concurso de normas.*

1. Siempre que no constituyan infracciones a la normativa general de protección de datos de carácter personal, los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de esta u otra ley orgánica se sancionarán observando las siguientes reglas:

a) El precepto especial se aplicará con preferencia al general.
b) El precepto más amplio o complejo absorberá el que sancione las infracciones subsumidas en aquel.
c) En defecto de los criterios anteriores, se aplicará el precepto que sancione los hechos con la sanción mayor.

2. En el caso de que un solo hecho constituya dos o más infracciones, o cuando una de ellas sea medio necesario para cometer la otra, la conducta será sancionada por aquella infracción a la que se aplique una mayor sanción.

SECCIÓN 2.ª INFRACCIONES

Artículo 25. *Clasificación de las infracciones.*

Las infracciones tipificadas en esta ley orgánica se clasifican en muy graves, graves y leves.

Artículo 26. *Infracciones muy graves.*

Constituyen infracciones muy graves:

a) La falta de remisión de los datos PNR, de acuerdo con lo establecido en el artículo 10.1 y 2, cuando se haya generado un riesgo grave para la seguridad ciudadana, la vida o la integridad física de las personas.
b) La falta de remisión de los datos PNR, conforme a los formatos y protocolos a los que se refiere el artículo 9.4, cuando se haya generado un riesgo grave para la seguridad ciudadana, la vida o la integridad física de las personas.
c) En caso de requerimiento previo, la falta de remisión de los datos PNR o la remisión fuera del plazo concedido al efecto, cuando se haya generado un riesgo grave para la seguridad ciudadana, la vida o la integridad física de las personas.
d) La falta de transmisión de los datos PNR a la UIP en los supuestos a los que se refiere el artículo 10.3.

Artículo 27. *Infracciones graves.*

Constituyen infracciones graves:

a) La falta de remisión de los datos PNR, de acuerdo con lo establecido en el artículo 10.1 y 2.
b) La falta de remisión de los datos PNR, conforme a los formatos y protocolos a los que se refiere el artículo 9.4.
c) La falta de adopción en tiempo y forma, por parte de los sujetos obligados, de las medidas necesarias para realizar legalmente las transmisiones.
d) En caso de requerimiento previo, la falta de remisión de los datos PNR o la remisión fuera del plazo establecido al efecto o sin cumplir con los requisitos técnicos y legales de transmisión.
e) Las omisiones en la transmisión de datos.

f) La falta de comunicación, conforme a lo dispuesto en esta ley orgánica, de cualquier cambio producido previamente o durante el trayecto, respecto al destino donde se tuviera previsto aterrizar.
g) La falta de diligencia en el mantenimiento de los sistemas electrónicos seguros de transmisión de los datos PNR siempre que no constituya infracción con arreglo a la normativa general de protección de datos de carácter personal.

Artículo 28. *Infracciones leves.*

Constituyen infracciones leves:

a) El incumplimiento de la obligación de informar a la UIP sobre los formatos de datos y protocolos de transmisión en el plazo previsto.
b) Cualquier otro incumplimiento de lo previsto en esta ley orgánica y que no constituya infracción grave o muy grave.

SECCIÓN 3.ª SANCIONES

Artículo 29. *Sanciones.*

Las infracciones muy graves serán sancionadas con multa de 60.001 a 300.000 euros; de 20.001 a 60.000 euros las graves; y de 3.000 a 20.000 euros las leves.

Artículo 30. *Graduación de las sanciones.*

Atendiendo al principio de proporcionalidad, se graduará la cuantía de las sanciones teniendo en cuenta, entre otras, las siguientes circunstancias, además de las previstas en el artículo 29 de la Ley 40/2015, de 1 de octubre:

a) La incidencia en la seguridad pública y/o en los derechos a la intimidad, la protección de datos, la imagen o el honor de las personas.
b) El beneficio económico obtenido como consecuencia de la comisión de la infracción.
c) La naturaleza, gravedad y duración de la infracción, teniendo en cuenta el número de afectados y los daños o perjuicios que hayan sufrido.
d) El grado de cooperación para poner remedio o mitigar los posibles efectos adversos.

Artículo 31. *Competencia sancionadora.*

Son órganos competentes para la imposición de las sanciones:

a) La persona titular del Ministerio del Interior, para la sanción de las infracciones muy graves.
b) La persona titular de la Secretaría de Estado de Seguridad, para la sanción de las infracciones graves y leves.

SECCIÓN 4.ª NORMAS ESPECIALES DE PROCEDIMIENTO SANCIONADOR

Artículo 32. *Medidas provisionales.*

Los gastos ocasionados por la adopción de las posibles medidas provisionales serán de cuenta del causante de los hechos objeto del procedimiento sancionador. Dichos gastos, en su caso, serán reclamables mediante el procedimiento administrativo de apremio cuando la sanción adquiera firmeza en vía administrativa.

Artículo 33. *Caducidad del procedimiento.*

El procedimiento caducará transcurrido un año desde su incoación sin que se haya notificado la resolución, debiendo, no obstante, tenerse en cuenta en el cómputo las posibles paralizaciones por causas

imputables al interesado o la suspensión que debiera acordarse por la existencia de un procedimiento judicial penal, cuando concurra identidad de sujeto, hecho y fundamento, hasta la finalización de este.

Artículo 34. *Acceso a los datos de otras Administraciones públicas.*

Los órganos competentes para imponer las sanciones previstas en esta ley orgánica podrán acceder, en el ejercicio de dichas competencias, a los datos relativos a los sujetos infractores que estén directamente relacionados con la investigación de los hechos constitutivos de infracción, con las debidas garantías de seguridad, integridad y disponibilidad. El acceso y el tratamiento posterior de los datos se realizarán, en todo caso, de conformidad con lo establecido en la normativa reguladora de protección de datos de carácter personal.

DISPOSICIONES ADICIONALES

Primera. *Plazo para comunicar los formatos de datos y protocolos de transmisión.*

Las compañías aéreas informarán a la UIP del formato de datos y del protocolo de transmisión que utilizarán, en el plazo de cuarenta días a contar desde la fecha de publicación en el «Boletín Oficial del Estado» de esta ley orgánica. El formato y el protocolo deberán estar entre los previstos en la Decisión de Ejecución (UE) 2017/759 de la Comisión, de 28 de abril de 2017.

Segunda. *Transmisión de datos PNR.*

Las transmisiones de datos PNR se realizarán según los medios de transmisión establecidos por la Secretaría de Estado de Seguridad, de acuerdo con lo dispuesto en el artículo 9.

Tercera. *Régimen jurídico del acceso por el Centro Nacional de Inteligencia a datos PNR.*

El acceso a los datos PNR por parte del Centro Nacional de Inteligencia y su control, se realizarán de acuerdo con lo previsto en esta ley orgánica, salvaguardando, en todo caso, el carácter de materia legalmente clasificada como secreto de sus actividades y objetivos, con el fin de dar cumplimiento a las misiones y funciones establecidas en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

Cuarta. *Transmisiones de datos PNR a las Direcciones Generales de la Policía y de la Guardia Civil y a las autoridades competentes de las Comunidades Autónomas que cuenten con un cuerpo de policía propio e integral.*

Las transmisiones de datos PNR a las Direcciones Generales de la Policía y de la Guardia Civil y su control, se realizarán de acuerdo con lo previsto en esta ley orgánica, salvaguardando, en todo caso, el carácter reservado de sus investigaciones y de la inteligencia generada en torno a dichos datos en relación a delitos de terrorismo y demás delitos graves.

Igual régimen de transmisión y salvaguarda de sus investigaciones e inteligencia que las contempladas en el párrafo anterior se aplicarán a las autoridades competentes de las Comunidades Autónomas que hayan asumido competencias para la protección de personas y bienes y para el mantenimiento de la seguridad ciudadana y cuenten con cuerpo de policía propio.

Quinta. *Transmisiones de datos PNR a la Dirección Adjunta de Vigilancia Aduanera.*

Las transmisiones de datos PNR a la Dirección Adjunta de Vigilancia Aduanera y su control, se harán de acuerdo con lo previsto en esta ley orgánica, salvaguardando, en todo caso, el carácter reservado de los datos con trascendencia tributaria, de acuerdo con la Ley 58/2003, de 17 de diciembre, General Tributaria, de sus investigaciones y de la inteligencia generada en torno a dichos datos en relación a delitos graves de su competencia.

Sexta. *Transmisiones de datos PNR a Jueces, Tribunales y Ministerio Fiscal.*

Las transmisiones de datos PNR a Jueces, Tribunales y Ministerio Fiscal se harán de acuerdo con lo previsto en esta ley orgánica, sin perjuicio de la aplicación a su tratamiento de la legislación reguladora del ejercicio de la potestad jurisdiccional.

En particular, las transmisiones de datos PNR a Jueces y Tribunales se efectuarán de acuerdo con lo previsto en el artículo 14.4 de esta ley orgánica.

DISPOSICIONES FINALES

Primera. *Título competencial.*

Esta ley orgánica se dicta al amparo de lo previsto en el artículo 149.1.1.ª y 29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales, y sobre la seguridad pública, respectivamente.

Segunda. *Preceptos que tienen carácter de ley orgánica.*

1. Tienen carácter orgánico los siguientes preceptos:

a) Los artículos 4 y 5.
b) El capítulo II.
c) La disposición final segunda.

2. Los preceptos no incluidos en el apartado anterior tienen carácter de ley ordinaria.

Tercera. *Incorporación de derecho de la Unión Europea.*

Mediante esta ley orgánica se incorpora al Derecho español la 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.

Cuarta. *Entrada en vigor.*

Esta ley orgánica entrará en vigor a los dos meses de su publicación en el «Boletín Oficial del Estado», excepto la disposición adicional primera, que entrará en vigor al día siguiente de dicha publicación.

Por tanto,
Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta ley orgánica.

Madrid, 16 de septiembre de 2020.

FELIPE R.

El Presidente del Gobierno,
PEDRO SÁNCHEZ PÉREZ-CASTEJÓN