

## I. DISPOSICIÓN XERAIS

### XEFATURA DO ESTADO

**10776** *Lei orgánica 1/2020, do 16 de setembro, sobre a utilización dos datos do Rexistro de Nomes dos Pasaxeiros para a prevención, detección, investigación e axuizamento de delitos de terrorismo e delitos graves.*

FELIPE VI

REI DE ESPAÑA

Saiban todos os que a viren e a entenderen que as Cortes Xerais aprobaron e eu sanciono a seguinte lei orgánica.

#### PREÁMBULO

##### I

A protección da vida e da seguridade dos cidadáns constitúe o obxectivo principal do espazo de liberdade, seguridade e xustiza da Unión Europea. Entre as medidas que se adoptaron para a súa consecución, o Consello da Unión Europea, a través do «Programa de Estocolmo: unha Europa aberta e segura que sirva e protexa o cidadán», do 4 de maio de 2010, instou a Comisión a presentar unha proposta sobre a utilización de datos do Rexistro de Nomes dos Pasaxeiros («Passenger Name Record», en diante PNR) para prever, detectar, investigar e axuizar os delitos de terrorismo e os delitos graves.

Así mesmo, no plano internacional veuse avanzando na dimensión exterior desta política da Unión Europea. A Comisión presentou unha serie de elementos esenciais desta na súa Comunicación do 21 de setembro de 2010 «Sobre o enfoque global das transferencias de datos dos rexistros de nomes dos pasaxeiros (PNR) aos terceiros países», e a Unión acadou diversos acordos internacionais con distintos Estados.

O incremento da ameaza do crime organizado e, especialmente, do terrorismo en Europa constitúen violacións moi graves dos valores universais da dignidade humana, a liberdade, a igualdade, a solidariedade e o desfrute dos dereitos humanos e das liberdades fundamentais en que se basea a Unión Europea. Co obxectivo de elevar os niveis de seguridade dos seus cidadáns e de crear un marco xurídico para a protección dos seus datos de carácter persoal, no que respecta ao seu tratamento polas autoridades competentes, adoptouse a Directiva (UE) 2016/681 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativa á utilización de datos do Rexistro de Nomes dos Pasaxeiros (PNR) para a prevención, detección, investigación e axuizamento dos delitos de terrorismo e da delincuencia grave.

Con este fin ínstanse os Estados membros a que introduzan nos seus ordenamentos internos as disposicións legais pertinentes para que os datos PNR dos voos exteriores da Unión Europea sexan transferidos a unha unidade de información sobre pasaxeiros que se cree en cada Estado, sen prexuízo de que se poida aplicar tamén aos voos interiores da Unión, segundo o criterio de cada país, como prevé a aludida Directiva (UE) 2016/681 do Parlamento Europeo e do Consello, do 27 de abril de 2016, posibilidade da cal se fai uso nesta lei orgánica.

Así mesmo, a Directiva (UE) 2016/681 do Parlamento Europeo e do Consello, do 27 de abril de 2016, exige a creación dun sistema uniforme na Unión Europea para o tratamento dos datos PNR, precisando claramente cales son estes, os fins a que se limita a súa recollida, a utilización e transmisión, o establecemento de unidades únicas de información sobre os pasaxeiros en cada Estado membro, así como a obrigatoriedade de adoptar medidas que faciliten que os operadores cumpran os seus deberes, incluída a

imposición de sancións efectivas, proporcionadas e disuasorias ante eventuais incumprimentos.

O tratamento dos datos PNR vai mellorar a resposta á ameaza do terrorismo e a delincuencia grave mediante o cotexo de tales datos coas bases de datos dispoñibles e pertinentes, para os efectos da prevención, detección, investigación e axuízamento de delitos de terrorismo e delitos graves, e a súa análise e avaliación utilizando uns criterios específicos e revisables periodicamente, que permitan a identificación de persoas que poidan estar relacionadas con este tipo de actividades criminais, ao tempo que minimizarán ao máximo o risco de afectar persoas inocentes.

## II

Esta lei orgánica estrutúrase en tres capítulos, trinta e catro artigos, seis disposicións adicionais e catro disposicións derradeiras.

O capítulo I establece as disposicións xerais.

O seu obxecto é regular, por un lado, a transferencia dos datos PNR por parte das compañías aéreas e outras entidades obrigadas; en segundo termo, a recollida, o tratamento e a protección deses datos, a súa transmisión ás autoridades competentes e o intercambio dos ditos datos con outros Estados membros, Europol e terceiros Estados; pola súa vez, a designación da Unidade de Información sobre Pasaxeiros española e, por último, o réxime sancionador.

Especifícanse os fins para os cales poden ser utilizados os datos PNR unicamente para previr, detectar, investigar e axuízar delitos de terrorismo e delitos graves.

O ámbito de aplicación inclúe, en principio, todos os voos internacionais que teñan orixe, destino ou tránsito en España, tanto de carácter comercial como privados, cunha serie de excepcións baseadas no tipo dos voos.

Excepcionalmente, como medida extraordinaria e sempre que existan indicios suficientes dunha contrastada situación de risco, poderanse suxeitar rutas ou voos concretos de ámbito nacional ao disposto nesta lei orgánica.

Así mesmo, defínense os suxeitos obrigados, diferenciando as compañías áreas das entidades de xestión de reservas de voos, cuxa incorporación nesta lei orgánica é unha posibilidade prevista na Directiva (UE) 2016/681 do Parlamento Europeo e do Consello, do 27 de abril de 2016.

Detérmínanse tamén os delitos de terrorismo e os demais delitos graves cuxa prevención, detección, investigación ou axuízamento xustifica a recollida dos datos PNR. Os delitos de terrorismo son os recollidos na Lei orgánica 10/1995, do 23 de novembro, do Código penal, como delitos das organizacións e grupos terroristas e delitos de terrorismo. En canto aos demais delitos graves, considérase como tales, para os efectos desta lei, aqueles castigados cunha pena de prisión igual ou superior a tres anos por seren constitutivos dalgúns dos enumerados no anexo II da Directiva (UE) 2016/681 do Parlamento Europeo e do Consello, do 27 de abril de 2016.

Por outro lado, especificáanse os datos dos pasaxeiros que deben ser enviados á Unidade de Información sobre Pasaxeiros, de entre os recompilados por parte dos suxeitos obrigados para os seus propios fins comerciais no transcurso normal da súa actividade. Entre estes figuran os datos contidos no sistema de información anticipada sobre pasaxeiros (sistema API), algúns dos cales, a diferenza dos anteriores, foron contrastados cos documentos oficiais de identificación.

Deberá enviarse tamén certa información sobre a tripulación correspondente aos datos API. Así mesmo, no caso dos voos privados deberanse enviar os ditos datos tanto dos pasaxeiros como dos tripulantes. É imprescindible, para conseguir as finalidades previstas na Directiva (UE) 2016/681 do Parlamento Europeo e do Consello, do 27 de abril de 2016, dispor de tales datos de tripulacións e de voos privados, sen os cales se poderían correr graves riscos de seguridade pública, como ten demostrado a experiencia dos últimos anos.

O capítulo II ocúpase do tratamento dos datos PNR.

Regúlase a Unidade de Información sobre Pasaxeiros española (UIP), incardinada na estrutura do Centro de Intelixencia contra o Terrorismo e o Crime Organizado dependente da Secretaría de Estado de Seguridade, órgano con experiencia en materia de coordinación e na recepción e análise da información estratéxica dispoñible na loita contra todo tipo de terrorismo e delincuencia organizada.

Determinanse as súas funcións, referidas tanto á recepción, ao tratamento e á análise dos datos PNR como ás comunicacións e intercambios destes coas autoridades competentes nacionais e unidades análogas doutros Estados membros, terceiros países e Europol.

Regúlase especificamente a figura do responsable de protección de datos, cuxa principal función será garantir a rigorosa observancia da lexislación vixente en materia de protección de datos de carácter persoal durante todo o proceso de recepción, tratamento, transmisión, conservación e supresión dos datos PNR.

A transmisión de datos levarase a cabo utilizando os formatos determinados e os protocolos definidos na Decisión de execución da Comisión UE 2017/759, do 28 de abril de 2017, relativa aos protocolos comúns e aos formatos de datos que deberán utilizar as compañías aéreas para a transmisión dos datos PNR ás unidades de información sobre pasaxeiros.

As compañías aéreas informarán a UIP do formato e protocolo de transmisión que utilizarán. Con respecto ás compañías aéreas que non dispoñan da infraestrutura técnica necesaria, prevese a posibilidade de acordar co Ministerio do Interior os medios electrónicos de transmisión, sempre que se respecten as garantías de seguridade.

Os datos serán enviados en dous momentos distintos: o primeiro, entre as corenta e oito e as vinte e catro horas anteriores á saída programada do voo, e o segundo producirase unha vez cerrado o voo, é dicir, no momento a partir do cal ninguén pode entrar no avión nin abandonalo. Se durante o voo se produce algunha modificación no destino, tamén deberá ser transmitida.

Cando sexa necesario acceder aos datos PNR para responder a unha ameaza real e concreta en momentos distintos aos anteriores, caso por caso, as compañías aéreas deberán transmitir á UIP os ditos datos con carácter inmediato ao requirimento recibido.

Sen prexuízo das obrigacións establecidas nesta lei orgánica, os tratamentos de datos de carácter persoal realizados polos suxeitos obrigados rexeranse polo disposto no Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos e pola lexislación interna que se dite en uso da habilitación contida naquel.

En relación co tratamento dos datos de carácter persoal por parte das autoridades competentes, estas estarán suxeitas ao deber de proporcionar ou pór á disposición do interesado a información e facilitar o exercicio dos dereitos deste recollidos na Directiva (UE) 2016/680 do Parlamento Europeo e do Consello, do 27 de abril de 2016, e na lei orgánica que a incorpore ao noso ordenamento interno.

Neste capítulo tamén se definen os propósitos para os cales a UIP realizará o tratamento dos datos PNR mediante a utilización dunha definida metodoloxía: avaliar as persoas a bordo da aeronave co fin de identificar aquelas que poidan ter relación con delitos de terrorismo ou delitos graves; revisar individualmente os resultados de tal avaliación previa automatizada; responder peticións das autoridades competentes ou de Europol e establecer criterios predeterminados que se utilizarán nesas avaliacións.

Para iso, a UIP cotexará os datos PNR coas bases de datos dispoñibles e pertinentes para os efectos da prevención, detección, investigación e axuizamento de delitos de terrorismo e delitos graves, e tratará os datos de acordo cos criterios predeterminados. Realizarse unha verificación automática *a priori* que, no caso de ofrecer un resultado positivo, requirirá necesariamente unha comprobación manual por parte dun especialista da propia UIP.

Precísase cales son as autoridades competentes que poden solicitar ou recibir datos PNR ou o resultado do tratamento deses datos por parte da UIP, co obxectivo de seguir examinando a dita información ou adoptar as medidas adecuadas para previr, detectar, investigar e axuizar delitos de terrorismo e delitos graves. Estas son as direccións xerais da Policía e da Garda Civil, o Centro Nacional de Intelixencia, a Dirección Adxunta de Vixilancia Alfandegueira e o Ministerio Fiscal. Tamén se consideran autoridades competentes as correspondentes das comunidades autónomas que asumisen estatutariamente competencias para a protección de persoas e bens e para o mantemento da seguridade cidadá e que contén cun corpo de policía propio. Os xuíces e tribunais, en garantía do principio de independencia constitucional, rexeranse, en canto ás peticións da dita información e á colaboración coa UIP, polo disposto na súa lexislación específica.

As peticións das autoridades competentes serán debidamente motivadas e con suficiente base. En ningún caso se admitirán peticións masivas e non fundamentadas. Todo tratamento que leven a cabo estas autoridades competentes sobre os datos recibidos da UIP será para os fins propios da loita contra os delitos de terrorismo e os delitos graves.

O capítulo recolle, ademais, unha serie de disposicións en materia de protección de datos, entre as cales figuran a obriga de conservación da documentación relativa aos sistemas e procedementos de tratamento; a obriga de rexistro das operacións de recollida, consulta, transferencia e supresión dos datos, así como a obriga de comunicar ao interesado e á autoridade nacional de control calquera violación dos datos persoais que dea lugar a un elevado risco para a protección deste ou afecte negativamente a intimidade do interesado.

Nunha Europa concibida como espazo de liberdade, seguridade e xustiza, a colaboración e cooperación entre os Estados membros cobra unha especial relevancia. E dentro desa cooperación, os aspectos relativos á seguridade tornáronse fundamentais nos últimos anos na loita contra o terrorismo e a criminalidade organizada. Nesa liña de colaboración, España poderá enviar datos PNR ou o resultado do seu tratamento a outros Estados membros, de oficio ou atendendo unha solicitude concreta. As peticións entre Estados deben ser motivadas e sempre orientadas ao cumprimento dos fins previstos nesta lei orgánica.

Prevese a posibilidade de que unha autoridade competente española se poida dirixir directamente á Unidade de Información sobre Pasaxeiros doutro Estado membro para unha solicitude de información, sempre que se dean conxuntamente as circunstancias de urxencia e imposibilidade de comunicación coa UIP nacional. En todo caso, remitírase copia da petición á UIP española.

A transferencia de datos a Europol levarase a cabo electronicamente e de forma motivada, sempre que entre no ámbito das súas competencias e sexa necesaria para o exercicio das súas funcións.

Inclúese o procedemento de transmisión de datos a terceiros países. Neste intercambio terase que observar o establecido na lexislación que traspoña a Directiva (UE) 2016/680 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativa á protección das persoas físicas no que respecta ao tratamento de datos persoais por parte das autoridades competentes para fins de prevención, investigación, detección ou axuizamento de infraccións penais ou de execución de sancións penais, e á libre circulación deses datos e pola que se derroga a Decisión marco 2008/977/JAI do Consello. Ademais, deberá tratarse dunha transmisión de datos necesaria para os fins desta lei orgánica, e o Estado receptor deles soamente poderá transmitilos, pola súa vez, a outro terceiro Estado se conta para iso coa expresa autorización da Unidade española. En todo caso, garantírase que a transmisión e a utilización de datos PNR a terceiros Estados manteñan uns estándares e garantías como os previstos nesta lei orgánica.

En garantía do dereito á intimidade dos suxeitos afectados e, en especial, do seu dereito á protección de datos de carácter persoal, prevese que os datos PNR facilitados á UIP polos suxeitos obrigados serán conservados durante cinco anos contados desde a súa transmisión. Unha vez transcorridos seis meses desde a súa recepción, os datos PNR que permitan a identificación directa do pasaxeiro serán despersonalizados mediante

enmascaramento, e só se permitirá o acceso á totalidade deles logo de aprobación da autoridade xudicial ou da persoa titular da Secretaría de Estado de Seguridade.

Cumprido o prazo dos cinco anos, serán suprimidos definitivamente, sen prexuízo da súa utilización por parte das autoridades competentes que os recibisen e que os estean a utilizar no marco dun asunto concreto para efectos de previr, detectar, investigar ou axuizar delitos de terrorismo ou delitos graves.

Por último, regúlanse neste capítulo as competencias da Axencia Española de Protección de Datos na súa condición de autoridade nacional de control de datos PNR.

O capítulo III, que regula o réxime sancionador, límitase a establecer as especialidades estritamente necesarias por razón da materia e, no demais, aplícase o réxime xeral previsto na Lei 39/2015, do 1 de outubro, do procedemento administrativo común das administracións públicas.

Así, defínense os suxeitos responsables, os réximes especiais de responsabilidade e o concurso de normas; tipifícanse as infraccións que se clasifican en moi graves, graves e leves; determínanse as sancións segundo a infracción de que se trate, para cuxa gradación se terán en conta a repercusión na seguridade pública, a gravidade ou o beneficio obtido, entre outras circunstancias; determínase a competencia sancionadora e, finalmente, inclúense as normas procedementais especiais sobre os gastos derivados da adopción de posibles medidas provisionais por parte do órgano competente para resolver, así como sobre a caducidade do procedemento.

Nas disposicións adicionais regúlase o prazo en que as compañías aéreas deberán comunicar á UIP o formato de datos e o protocolo de transmisión que utilizarán; establécese que as comunicacións se farán segundo os procedementos establecidos pola Secretaría de Estado de Seguridade, e establécense normas referentes á transmisión dos datos PNR remitidos a determinadas autoridades competentes como son o Centro Nacional de Intelixencia, as direccións xerais da Policía e da Garda Civil, a Dirección Adxunta de Vixilancia Alfandegueira e os xuíces e tribunais e o Ministerio Fiscal.

Ademais, contén catro disposicións derradeiras, relativas ao título competencial, aos preceptos que teñen carácter de lei orgánica, á incorporación de dereito da Unión Europea e á entrada en vigor.

### III

Na elaboración desta lei orgánica observáronse os principios de necesidade, eficacia, proporcionalidade, seguridade xurídica, transparencia e eficiencia, de acordo co artigo 129 da Lei 39/2015, do 1 de outubro. Trátase dunha norma necesaria para a transposición da Directiva (UE) 2016/681 do Parlamento Europeo e do Consello, do 27 de abril de 2016, cuxa aprobación goza das garantías correspondentes ao rango de lei orgánica por supor un desenvolvemento de dereitos fundamentais dos cidadáns.

Por último, está incluída no Plan anual normativo para 2018 aprobado polo Consello de Ministros na súa reunión do 7 de decembro de 2017.

## CAPÍTULO I

### Disposicións xerais

#### Artigo 1. *Obxecto.*

1. Esta lei orgánica, co propósito de garantir e protexer a vida e a seguridade dos cidadáns, ten por obxecto regular:

a) A transferencia de datos do Rexistro de Nomes dos Pasaxeiros (en diante, datos PNR), así como da información da tripulación referida no artigo 5.3, correspondentes a voos internacionais e, se é o caso, nacionais, nos termos e para os efectos previstos no capítulo II.

b) O sistema de recollida, uso, almacenamento, tratamento, protección, acceso e conservación dos datos PNR, a transmisión de tales datos ás autoridades competentes, así como o seu intercambio cos Estados membros da Unión Europea, con Europol e con terceiros países.

c) A determinación e atribución das funcións da Unidade de Información sobre Pasaxeiros española.

d) O réxime sancionador aplicable ás infraccións de conformidade co disposto nesta lei orgánica.

2. Os datos PNR poderán ser obxecto de tratamento unicamente coa finalidade de previr, detectar, investigar e axuizar os delitos de terrorismo e os delitos graves que se enumeran no artigo 4, e de acordo cos propósitos establecidos no artigo 12.2.

#### Artigo 2. *Ámbito de aplicación.*

1. Esta lei orgánica será de aplicación, en todo caso, aos datos PNR correspondentes ás persoas que viaxen nos voos internacionais, tanto interiores coma exteriores da Unión Europea, coa súa saída do territorio español ou chegada a el, ou que fagan escala nel. Neste último suposto, sempre se entenderán comprendidos os pasaxeiros en tránsito ou en conexión, coas precisións establecidas no punto seguinte.

2. O seu ámbito de aplicación esténdese aos voos comerciais e aos voos privados.

Non será de aplicación aos voos realizados por aeronaves de Estado e por aeronaves privadas, fretadas polo Estado para a prestación ou apoio de servizos de interese militar e, en xeral, servizos estatais non comerciais, durante os voos dedicados exclusivamente a materializar tal prestación ou apoio, que se asimilarán ás aeronaves de Estado, aos traballos aéreos, á aviación xeral que non teña por obxecto o transporte de persoas, aos servizos aeroportuarios, aos servizos de navegación aérea, aos voos relacionados coa produción de aeronaves civís, aos voos de adestramento de tripulacións, aos voos de traslado para mantemento e revisión e aos voos relacionados con funcións regulatorias.

3. Como medida extraordinaria e polo tempo que resulte imprescindible, será de aplicación ás rutas ou aos voos concretos nacionais que non efectúen escalas en ningún outro Estado, sempre que existan indicios suficientes dunha clara e contrastada situación de risco, coa finalidade de previr, detectar, investigar e axuizar os delitos a que se refire o artigo 4.

A determinación de tales rutas ou voos será acordada polo Consello de Ministros, por proposta do titular do Ministerio do Interior, tendo en conta o carácter extraordinario da medida, a súa necesidade e proporcionalidade.

#### Artigo 3. *Suxeitos obrigados.*

1. Son suxeitos obrigados as compañías aéreas, entendendo como tales as empresas de transporte aéreo cunha licenza de explotación válida ou similar para o transporte por vía aérea.

Para os efectos desta lei orgánica, a definición de empresa será a establecida no Regulamento (CE) 1008/2008 do Parlamento Europeo e do Consello, do 24 de setembro de 2008, sobre normas comúns para a explotación de servizos aéreos na Comunidade, e comprende calquera persoa física ou xurídica, con ou sen fins de lucro, ou calquera organismo oficial dotado ou non de personalidade xurídica propia.

No caso dos voos privados, serán suxeitos obrigados os operadores das aeronaves, ben sexa como propietarios, arrendatarios ben en virtude doutro título posesorio recoñecido pola lexislación vixente.

2. Son igualmente suxeitos obrigados as entidades de xestión de reserva de voos, entendendo como tales as entidades que xestionen reservas de voos de pasaxeiros e soliciten datos PNR deles, calquera que sexa o medio utilizado para iso, tales como os operadores turísticos ou as axencias de viaxes, que estarán obrigadas nos termos previstos no artigo 9.2.

Artigo 4. *Delitos de terrorismo e delitos graves.*

1. Para os exclusivos efectos desta lei orgánica, son delitos de terrorismo os recollidos na Lei orgánica 10/1995, do 23 de novembro, do Código penal, como delitos das organizacións e grupos terroristas e delitos de terrorismo.

2. Así mesmo, para os exclusivos efectos desta lei orgánica, son delitos graves aqueles que a lei castigue cunha pena de prisión igual ou superior a tres anos por seren constitutivos de:

- a) Pertenza a unha organización delituosa.
- b) Trata de seres humanos.
- c) Explotación sexual de nenos e pornografía infantil.
- d) Tráfico ilícito de estupefacientes e substancias psicotrópicas.
- e) Tráfico ilícito de armas, municións e explosivos.
- f) Corrupción.
- g) Fraude, incluída a que afecte os intereses financeiros da Unión Europea.
- h) Branqueo do produto do delito e falsificación de moeda, con inclusión do euro.
- i) Delitos informáticos/ciberdelincuencia.
- j) Delitos contra o ambiente, incluído o tráfico ilícito de especies animais protexidas e de especies e variedades vexetais protexidas.
- k) Axuda á entrada e residencia ilegais.
- l) Homicidio voluntario, agresión con lesións graves.
- m) Tráfico ilícito de órganos e tecidos humanos.
- n) Secuestro, detención ilegal e toma de reféns.
- ñ) Roubo organizado e a man armada.
- o) Tráfico ilícito de bens culturais, incluídas as antigüidades e as obras de arte.
- p) Falsificación e violación de dereitos de propiedade intelectual ou industrial de mercadorías.
- q) Falsificación de documentos administrativos e tráfico de documentos administrativos falsos.
- r) Tráfico ilícito de substancias hormonais e outros factores de crecemento.
- s) Tráfico ilícito de materiais radioactivos ou substancias nucleares.
- t) Violación.
- u) Delitos incluídos na xurisdición da Corte Penal Internacional.
- v) Secuestro de aeronaves e buques.
- w) Sabotaxe.
- x) Tráfico de vehículos roubados.
- y) Espionaxe industrial.

Artigo 5. *Datos do Rexistro de Nomes dos Pasaxeiros (datos PNR).*

1. Os datos PNR son o conxunto de datos relativos á viaxe dun pasaxeiro, reservada por el ou no seu nome, que recolle a información necesaria para a xestión da reserva.

2. Os datos PNR relativos aos pasaxeiros son os seguintes:

- a) Localizador de rexistro PNR.
- b) Data de reserva e de emisión do billete.
- c) Datas previstas da viaxe.
- d) Nomes e apelidos.
- e) Enderezo e datos de contacto (número de teléfono, enderezo de correo electrónico).
- f) Todos os datos de pagamento, incluído o enderezo de facturación.
- g) Itinerario completo da viaxe para o PNR específico.
- h) Información sobre viaxeiros frecuentes.
- i) Axencia de viaxes ou operador de viaxes.
- j) Situación de voo do pasaxeiro: confirmacións, facturación, non comparecencia ou pasaxeiros de última hora sen reserva.

- k) Información PNR escindida ou dividida.
- l) Observacións xerais, incluída toda a información dispoñible sobre menores de dezoito anos non acompañados, como nome, apelidos e sexo do menor, idade, idiomas que fala, nome, apelidos e enderezo de contacto do acompañante no aeroporto de saída e vínculo co menor, nome, apelidos e enderezo de contacto do acompañante no aeroporto de chegada e vínculo co menor, axente no lugar de saída e de chegada.
- m) Información sobre o billete, incluídos o número do billete, a data de emisión, os billetes só de ida e a indicación da tarifa dos billetes electrónicos (*Automatic Ticket Fare Quote*).
- n) Datos do asento, incluído o número.
- ñ) Información sobre códigos compartidos.
- o) Toda a información relativa á equipaxe.
- p) Número de viaxeiros e outros nomes de viaxeiros que figuran no PNR.
- q) Calquera información recollida no sistema de información anticipada sobre os pasaxeiros (sistema API), incluídos o tipo, número, país de emisión e data de expiración de calquera documento de identidade, nacionalidade, apelidos, nome, sexo, data de nacemento, compañía aérea, número de voo, data de saída, data de chegada, aeroporto de saída, aeroporto de chegada, hora de saída e hora de chegada.
- r) Todo o historial de cambios dos datos PNR indicados nas alíneas a) a q).

3. No caso dos voos comerciais, as disposicións desta lei orgánica serán aplicables, ademais de aos datos dos pasaxeiros, aos datos da tripulación no caso da alínea q) e aos datos de calquera outra persoa a bordo sinalados nas alíneas o) e q) do punto anterior. Igualmente, no caso dos voos privados, serán de aplicación a tales datos dos pasaxeiros e tripulantes.

## CAPÍTULO II

### Tratamento dos datos PNR

#### Artigo 6. *Unidade de Información sobre Pasaxeiros.*

1. A Unidade de Información sobre Pasaxeiros española (UIP) intégrase organicamente no Centro de Intelixencia contra o Terrorismo e o Crime Organizado, dependente da Secretaría de Estado de Seguridade do Ministerio do Interior.
2. A UIP é a responsable do tratamento dos datos PNR.

#### Artigo 7. *Funcións e facultades.*

1. A UIP realizará exclusivamente as seguintes funcións:
  - a) Recoller os datos PNR, almacenalos, tratalos e transferir, se é o caso, tales datos ou o resultado do seu tratamento ás autoridades competentes.
  - b) Intercambiar tanto os datos PNR como o resultado do seu tratamento coas unidades de información sobre pasaxeiros doutros Estados membros da Unión Europea, con Europol e con terceiros países.
2. Para a realización das funcións mencionadas no punto anterior, a UIP será responsable de:
  - a) Analizar, relacionar e valorar os datos obtidos.
  - b) Establecer e actualizar criterios útiles para identificar as persoas que poidan estar implicadas en delitos de terrorismo e delitos graves, en cooperación, se é o caso, coas autoridades competentes.



- c) Elaborar informes de intelixencia estratéxica e de análise de risco.
- d) Colaborar coas autoridades competentes encargadas das investigacións e actuacións operativas, así como elaborar os protocolos de actuación pertinentes en colaboración con estas.
- e) Pór os feitos que poidan ser constitutivos das infraccións previstas nesta lei orgánica en coñecemento do órgano competente para sancionalas.
- f) Elaborar estatísticas anuais sobre a súa actividade, incluíndo o número total de persoas cuxos datos PNR fosen recompilados e intercambiados, así como o número de persoas identificadas para un exame ulterior.

3. O almacenamento, o tratamento e a análise dos datos PNR levaranse a cabo exclusivamente nun ou en varios lugares seguros dentro do territorio nacional.

4. Cando for preciso para desenvolver as súas funcións, o persoal ao servizo das autoridades competentes enumeradas no artigo 14 poderá prestar servizos na UIP. Este persoal continuará en servizo activo no seu corpo e dependerá orgánica, funcional e retributivamente da súa Administración de orixe, sen prexuízo de que no desenvolvemento das súas funcións na UIP deba atermos ao preceptuado para esta respecto á súa organización e funcionamento.

#### Artigo 8. *Responsable de protección de datos.*

1. A UIP designará unha persoa como responsable de protección dos datos PNR, que velará por que se adopten as medidas oportunas para controlar o tratamento destes datos e por que se apliquen as garantías en materia de protección de datos. O responsable de protección de datos actuará como punto de contacto único, ao cal calquera interesado terá dereito a dirixirse para todas as cuestións relativas ao tratamento dos seus datos PNR.

2. A persoa designada serao atendendo ás súas calidades profesionais e, en particular, aos seus coñecementos especializados da lexislación e das prácticas en materia de protección de datos persoais, e á súa capacidade para desempeñar as funcións recollidas nesta lei orgánica. Deberá contar cos medios necesarios para desempeñar as súas funcións de maneira eficaz e independente.

3. A persoa responsable da protección de datos terá acceso a todos os datos PNR tratados pola UIP. Se considera que o tratamento dun dato non foi lícito, porao en coñecemento do responsable do tratamento para que se adopten as medidas correctoras necesarias e, se o coida oportuno, poderá remitir o asunto á autoridade nacional de control.

4. No non previsto nesta lei orgánica rexerese polo regulado para os delegados de protección de datos na lexislación que traspoña a Directiva (UE) 2016/680 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativa á protección das persoas físicas no que respecta ao tratamento de datos persoais por parte das autoridades competentes para fins de prevención, investigación, detección ou axuizamento de infraccións penais ou de execución de sancións penais, e á libre circulación deses datos e pola que se derroga a Decisión marco 2008/977/JAI do Consello, e ata ese momento polas normas que regulen no dereito español o tratamento de datos persoais por parte das autoridades competentes para fins de prevención, investigación, detección e axuizamento de infraccións penais ou de execución de sancións penais.

#### Artigo 9. *Obrigacións de transmisión de datos.*

1. As compañías aéreas enviarán os datos PNR correspondentes aos voos comprendidos no artigo 2, que recompilasen no transcurso normal da súa actividade, á base de datos da UIP. No caso dos voos privados, o operador asumirá a responsabilidade de que a información prevista no artigo 5.3 sexa remitida á UIP.

No caso de que existan varias compañías aéreas relacionadas cun mesmo voo, a obrigaçión de transmitir os datos recaerá na compañía aérea que actúe como operadora deste.

2. As entidades de xestión de reservas de voos introducirán no PNR os datos que recompilasen no transcurso normal da súa actividade respecto aos voos comprendidos no artigo 2.

3. No cumprimento das súas obrigaçións de información, e sen prexuízo do establecido no Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento dos seus datos persoais e á libre circulación destes datos e na lexislación interna que se dite en uso da habilitación contida naquel, os suxeitos obrigados informarán as persoas a que se refiran os datos PNR do motivo da súa recollida e do seu destinatario, a Unidade de Información sobre Pasaxeiros, ante cuxo responsable de protección de datos poderán dirixirse para todas as cuestións relativas ao tratamento dos seus datos PNR.

4. As compañías aéreas enviarán os datos PNR á UIP, utilizando en todo caso medios electrónicos que ofrezan garantías suficientes en relación coas medidas de seguridade técnicas e as medidas organizativas que rexen o tratamento de datos que se vai levar a cabo. Esta transmisión realizarase consonte un dos formatos de datos e mediante un dos protocolos de transmisión establecidos na Decisión de execución da Comisión (UE) 2017/759, do 28 de abril de 2017, relativa aos protocolos comúns e aos formatos de datos que deberán utilizar as compañías aéreas para a transmisión dos datos PNR ás unidades de información sobre pasaxeiros.

No caso de que transmitan datos API sobre os pasaxeiros de maneira separada respecto do resto dos datos PNR para o mesmo voo, deberán utilizar, para o seu envío á UIP, o formato específico de datos que se recolle na Decisión de execución da Comisión (UE) 2017/759, do 28 de abril de 2017.

En caso de fallo técnico ou imposibilidade sobrevida, realizarán a transmisión dos datos PNR, no prazo máis breve posible, por calquera outro medio apropiado que garanta un nivel adecuado de seguridade dos ditos datos.

5. As compañías aéreas que non operen voos consonte un calendario concreto e público e que non dispoñan da infraestrutura técnica necesaria para usar os formatos de datos e os protocolos de transmisión incluídos na Decisión de execución da Comisión (UE) 2017/759, do 28 de abril de 2017, utilizarán, para a transmisión dos datos PNR, os formatos e os medios electrónicos que se acorden de forma bilateral entre a compañía aérea e o Ministerio do Interior, sempre que ofrezan garantías suficientes respecto das medidas de seguridade técnicas. Este réxime será o aplicable en todo caso aos voos privados.

#### Artigo 10. *Momentos da transmisión de datos.*

1. Os momentos en que as compañías aéreas deben transmitir os datos PNR á UIP serán os seguintes:

- a) Entre as vinte e catro e as corenta e oito horas antes da hora de saída programada do voo, e
- b) inmediatamente despois do peche do voo, unha vez que os pasaxeiros embarcasen no avión en preparación da saída e non sexa posible embarcar ou desembarcar.

As compañías aéreas poderán limitar esta transmisión prevista na alínea b) ás actualizacións da información transmitida conforme a alínea a).

2. As compañías aéreas deberán comunicar calquera cambio producido previamente ou durante o traxecto, respecto ao destino onde se tivese previsto aterrizar ou á realización dunha escala non programada.

3. Ademais, cando sexa necesario acceder aos datos PNR para responder a unha ameaza real e concreta relacionada con delitos de terrorismo ou con delitos graves, en momentos distintos dos previstos no punto 1, todos os suxeitos obrigados, caso por caso, deberán transmitir á UIP os ditos datos con carácter inmediato ao requirimento recibido.

Artigo 11. *Réxime xurídico aplicable ao tratamento de datos PNR.*

1. Os tratamentos de datos de carácter persoal que leven a cabo a UIP e as autoridades competentes referidas no artigo 14 rexeranse por esta lei orgánica e, supletoriamente, pola lexislación que traspoña a Directiva (UE) 2016/680 do Parlamento Europeo e do Consello, do 27 de abril de 2016, e ata ese momento polas normas que regulen no dereito español o tratamento de datos persoais por parte das autoridades competentes para fins de prevención, investigación, detección e axuizamento de infraccións penais ou de execución de sancións penais. Neste réxime xurídico inclúense a protección dos datos persoais dos pasaxeiros e os seus dereitos de acceso, rectificación, supresión, limitación do tratamento, indemnización e recurso xudicial.

2. Sen prexuízo das obrigacións establecidas nesta lei orgánica, os tratamentos de datos de carácter persoal realizados polos suxeitos obrigados referidos no artigo 3 rexeranse polo disposto no Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, do 27 de abril de 2016, e pola lexislación interna que se dite en uso da habilitación contida naquel.

Artigo 12. *Tratamento dos datos PNR.*

1. Os datos PNR serán recollidos pola UIP.

Se a información transmitida inclúe datos distintos dos relacionados nesta lei orgánica, a UIP suprimiráos inmediatamente e de maneira definitiva no momento da súa recepción.

2. A UIP tratará os datos PNR só para os seguintes propósitos:

a) Realizar unha avaliación dos pasaxeiros e da tripulación antes da chegada ou saída programada do voo, co fin de identificar as persoas que deban ser examinadas de novo polas autoridades competentes e, se é o caso, por Europol ante a posibilidade de poderen estar implicadas nun delito de terrorismo ou nun delito grave.

b) Responder en cada caso particular ás peticións das autoridades competentes, debidamente motivadas e con suficiente base, para que lles transfiran datos PNR en supostos específicos para efectos de prevención, detección, investigación e axuizamento de delitos de terrorismo e delitos graves, así como o resultado do seu tratamento.

c) Analizar os datos PNR co fin de establecer ou actualizar criterios que se deben utilizar nas avaliacións realizadas en virtude do punto 3.b), co obxecto de identificar as persoas que poidan estar implicadas en delitos de terrorismo ou delitos graves.

Estes criterios de avaliación predeterminados deberán ser proporcionados e específicos e estar orientados á finalidade que perseguen. Non se basearán na orixe racial ou étnica, nas opinións políticas, nas crenzas relixiosas ou filosóficas, na pertenza a un sindicato ou partido político, na saúde ou na vida ou orientación sexual da persoa. A UIP establecerá e revisará periodicamente estes criterios, en colaboración coas autoridades competentes.

3. Ao realizar a avaliación a que se refire o punto 2.a), a UIP poderá someter os datos PNR ás seguintes operacións:

a) Comparará os datos PNR con todas as bases de datos dispoñibles e pertinentes, para os efectos da prevención, detección, investigación e axuizamento de delitos de terrorismo e delitos graves.

b) Tratará os datos PNR de acordo cos criterios predeterminados establecidos para identificar as persoas que poidan estar implicadas en delitos de terrorismo ou en delitos graves.

4. Cando a avaliación efectuada de acordo co punto 2.a) amose un resultado positivo, a UIP procederá á revisión individual de tal resultado a través de medios non automatizados, co fin de comprobar a necesidade de que as autoridades competentes realicen un exame ulterior ou emprendan as accións ou inicien os procedementos oportunos. Para tal fin, a UIP deberá transmitir os datos PNR ás autoridades competentes.

#### Artigo 13. *Consecuencias da avaliación.*

As consecuencias das avaliacións dos pasaxeiros a que se refire o punto 2.a) do artigo anterior non prexudicarán o dereito de entrada en España das persoas que gocen do dereito de libre circulación na Unión Europea.

Cando estas avaliacións se efectúen en relación con pasaxeiros de voos interiores da Unión Europea aos cales lles sexa aplicable o Regulamento (UE) 2016/399 do Parlamento Europeo e do Consello, do 9 de marzo de 2016, polo que se establece un Código de normas da Unión para o cruzamento de persoas polas fronteiras, as consecuencias axustaranse ao previsto no dito regulamento.

#### Artigo 14. *Autoridades competentes.*

1. As autoridades competentes para solicitar ou recibir da UIP datos PNR ou o resultado do tratamento de tales datos co fin de seguir examinando esa información ou de adoptar as medidas adecuadas para previr, detectar, investigar e axuizar delitos de terrorismo e delitos graves serán as seguintes:

- a) A Dirección Xeral da Policía.
- b) A Dirección Xeral da Garda Civil.
- c) O Centro Nacional de Intelixencia.
- d) A Dirección Adxunta de Vixilancia Alfandegueira.
- e) O Ministerio Fiscal.
- f) As correspondentes das comunidades autónomas que asumisen estatutariamente competencias para a protección de persoas e bens e para o mantemento da seguridade cidadá, e que contén cun corpo de policía propio.

2. As peticións de datos realizadas polas autoridades competentes serán debidamente motivadas e con suficiente base. En ningún caso se admitirán peticións masivas e non fundamentadas.

3. As autoridades competentes colaborarán coa UIP, no ámbito das súas competencias, para o cumprimento dos fins desta lei orgánica.

4. Aos xuíces e tribunais, que terán a consideración de autoridades competentes, non lles serán de aplicación os puntos 2 e 3, en atención ao principio constitucional de independencia do poder xudicial e, en canto ás peticións de datos e á colaboración coa UIP, rexeranse polo que estableza a lexislación aplicable ao exercicio da función xurisdiccional.

5. Os datos remitidos pola UIP ás autoridades competentes poderán ser obxecto de tratamento posterior por parte destas, unicamente cos fins específicos de prevención, detección, investigación e axuizamento de delitos de terrorismo e delitos graves, sen prexuízo das accións ou procedementos que se poidan realizar ou iniciar no caso de que, como consecuencia do tratamento de tales datos, se detecten outros delitos ou indicios deles.

6. As autoridades competentes non adoptarán ningunha decisión que produza efectos xurídicos adversos para unha persoa ou que afecte negativamente unha persoa unicamente en razón do tratamento automatizado de datos PNR.

Estas decisións non se deberán basear na orixe racial ou étnica, nas opinións políticas, nas crenzas relixiosas ou filosóficas, na pertenza a un sindicato ou partido político, na saúde ou na vida e orientación sexual da persoa.

Artigo 15. *Protección dos datos de carácter persoal.*

1. A UIP non poderá tratar datos PNR que revelen a orixe racial ou étnica, as opinións políticas, as crenzas relixiosas ou filosóficas, a pertenza a un sindicato ou partido político, a saúde, a vida ou a orientación sexual da persoa. No caso de que reciba datos PNR que revelen tal información, suprimiraos inmediatamente.

2. A UIP conservará a documentación relativa a todos os sistemas e procedementos de tratamento baixo a súa responsabilidade.

Esta documentación constará, como mínimo, dos seguintes elementos:

a) Os datos identificativos do persoal da UIP encargado do tratamento dos datos PNR, así como do responsable de protección de datos, e os distintos niveis de autorización de acceso.

b) As solicitudes cursadas polas autoridades competentes e polas unidades de información sobre pasaxeiros doutros Estados membros.

c) Todas as solicitudes e transmisións de datos PNR a un terceiro país ou a Europol.

A UIP porá esta documentación á disposición da autoridade nacional de control por petición desta, de acordo coa lexislación vixente.

3. A UIP levará rexistros, ao menos, das operacións de recollida, consulta, transferencia e supresión dos datos.

Os rexistros de consulta e transferencia mostrarán, en particular, a finalidade, a data e a hora de tales operacións e, na medida do posible, a identidade da persoa que consultou ou transmitiu os datos PNR e a identidade dos receptores dos ditos datos.

Os rexistros utilizaranse exclusivamente para efectos de verificación, autocontrol, e garantía da integridade dos datos e da súa seguridade ou de auditoría. Estes rexistros conservaranse por un período de cinco anos.

A UIP porá os rexistros á disposición da autoridade nacional de control por petición desta, de acordo coa lexislación aplicable.

4. Cando sexa probable que unha violación dos datos persoais dea lugar a un elevado risco para a protección destes ou afecte negativamente a intimidade do interesado, a UIP comunicará, sen demora inxustificada, tal violación ao interesado e á autoridade nacional de control.

5. A UIP aplicará as medidas e os procedementos técnicos e organizativos adecuados para garantir un elevado nivel de seguridade correspondente aos riscos que entrañen o tratamento e as características dos datos PNR.

Artigo 16. *Intercambio de información entre Estados membros da Unión Europea.*

1. A UIP transmitirá os datos PNR pertinentes e necesarios ou o resultado do seu tratamento, relativos ás persoas identificadas por ela como persoas que poidan estar implicadas nun delito de terrorismo ou nun delito grave, ás unidades de información sobre pasaxeiros dos outros Estados membros. Esta transmisión só se levará a cabo tras unha análise de cada caso e, en supostos de tratamento automatizado dos datos PNR, tras unha revisión individualizada por medios non automatizados.

En caso de que a UIP reciba datos PNR ou o resultado do seu tratamento da Unidade de Información sobre Pasaxeiros doutro Estado membro, deberá proporcionar todos os datos pertinentes e necesarios ás autoridades competentes correspondentes, tras unha revisión individualizada.

2. A UIP terá dereito a solicitar á Unidade de Información sobre Pasaxeiros de calquera outro Estado membro, en cada caso concreto, para a prevención, detección, investigación ou axuízamento de delitos de terrorismo ou delitos graves, que lle subministre os datos PNR almacenados na súa base de datos e que non fosen despersonalizados mediante enmascaramento de elementos dos datos, así como, se for necesario, o resultado de calquera tratamento destes. A solicitude deberá ser debidamente motivada.

No caso de que fosen despersonalizados mediante enmascaramento de elementos de datos, a transmisión terá lugar de conformidade co dereito nacional aplicable no Estado membro da Unidade de Información sobre Pasaxeiros requirida.

3. Pola súa vez, a Unidade de Información sobre Pasaxeiros de calquera Estado membro poderá solicitar directamente á UIP datos PNR ou o resultado do seu tratamento, baixo as mesmas condicións previstas no punto anterior. Nese caso, a UIP proporcionará a información solicitada o antes posible.

No suposto de que os datos requiridos fosen despersonalizados mediante enmascaramento, a UIP unicamente proporcionará os datos completos ou o resultado do seu tratamento ante casos específicos cando sexa necesario para a prevención, detección, investigación e axuizamento de delitos de terrorismo e delitos graves, e só cando o autorizase a autoridade xudicial ou a persoa titular da Secretaría de Estado de Seguridade.

4. As autoridades competentes que requiran datos PNR solicitados por un Estado membro da Unión Europea canalizarán as súas solicitudes de forma motivada a través da UIP.

Unicamente cando non sexa posible dirixir as súas peticións a través da UIP e en caso de urxencia, e sempre que a solicitude cumpra coas condicións establecidas no punto 2, as autoridades competentes poderán solicitar eses datos directamente á Unidade de Información sobre Pasaxeiros doutro Estado membro.

Destas solicitudes directas e urxentes remitirase copia á UIP, ao mesmo tempo que á Unidade de Información sobre Pasaxeiros do Estado membro de que se trate, coa cal se deberá achegar, o antes posible, unha motivación da remisión directa.

5. De maneira excepcional, cando sexa necesario acceder aos datos PNR para responder a unha ameaza concreta e real relacionada con delitos de terrorismo ou delitos graves, a UIP solicitará á Unidade de Información sobre Pasaxeiros do Estado membro correspondente que acceda aos datos PNR fóra dos momentos ordinarios de transmisión establecidos no artigo 10 e que llos transmita.

Do mesmo modo, a UIP dará resposta o antes posible ás solicitudes que reciba doutros Estados membros nos supostos previstos no parágrafo anterior.

6. O intercambio de información previsto neste artigo poderase realizar utilizando calquera das vías existentes de cooperación entre as autoridades competentes dos Estados membros.

#### Artigo 17. *Transferencia de datos a Europol.*

1. A UIP transferirá os datos PNR específicos ou o resultado do seu tratamento solicitados por Europol, caso por caso, de forma electrónica e debidamente motivada, cando sexa estritamente necesario para apoiar e reforzar a acción dun Estado membro da Unión Europea para efectos de previr, detectar, investigar ou axuizar delitos de terrorismo ou delitos graves, sempre que o delito entre no ámbito de competencias de Europol e para o desempeño das súas funcións.

2. A solicitude indicará as causas razoables polas cales Europol considera que a transmisión dos datos PNR ou dos resultados do seu tratamento vai contribuír significativamente a previr, detectar ou investigar a infracción penal en cuestión.

3. Europol informará o responsable da protección de datos de cada un dos intercambios de información en virtude deste artigo.

4. O intercambio de información realizarase a través da Rede de intercambio seguro de información (SIENA).

#### Artigo 18. *Transferencias de datos a terceiros países non membros da Unión Europea.*

1. A UIP poderá transferir a terceiros países non membros da UE datos PNR, así como o resultado do seu tratamento, en casos concretos e se se cumpren concorrentemente os seguintes requisitos:

a) As condicións establecidas para as transferencias de datos a terceiros países na lexislación que traspoña a Directiva (UE) 2016/680 do Parlamento Europeo e do Consello,

do 27 de abril de 2016, e ata ese momento polas normas que regulen no dereito español o tratamento de datos persoais por parte das autoridades competentes para fins de prevención, investigación, detección e axuizamento de infraccións penais ou de execución de sancións penais.

- b) A transmisión resulta necesaria para os fins sinalados no artigo 1.2.
- c) O terceiro país comprométese a transmitir os datos PNR a outro terceiro país só se for estritamente necesario para os fins desta lei orgánica e sempre contando coa autorización expresa da UIP.
- d) Os previstos no artigo 16.

2. As transmisións de datos PNR pola UIP sen consentimento previo do Estado membro do cal se obtiveron permitíranse en circunstancias excepcionais e unicamente se:

- a) Son esenciais para responder a unha ameaza específica e real relacionada con delitos de terrorismo ou delitos graves dun Estado membro ou dun terceiro país e
- b) o consentimento previo non se puido obter ao seu debido tempo.

A UIP informará sen demora a autoridade do Estado membro responsable de dar o consentimento. A transmisión será rexistrada pola UIP e poderá ser obxecto dunha verificación posterior.

3. Cada vez que a UIP transfira datos PNR a terceiros países en virtude do previsto neste artigo, o seu responsable de protección de datos será informado.

4. A UIP exclusivamente transmitirá datos PNR ás autoridades competentes de terceiros países tras asegurarse de que se axustan a un estándar de condicións e garantías equivalente ao desta lei orgánica e de que a utilización dos datos PNR prevista polos receptores se axusta ás ditas condicións e garantías.

#### Artigo 19. *Período de conservación dos datos e despersonalización.*

1. Os datos PNR proporcionados á UIP polos suxeitos obrigados conservaranse nunha base de datos da Unidade durante un prazo de cinco anos a partir da data da súa transmisión á UIP.

2. Transcorrido un prazo de seis meses desde a transmisión a que se refire o punto 1, todos os datos PNR deberán ser despersonalizados mediante enmascaramento, de maneira que resulten invisibles para un usuario os seguintes elementos que servirían para identificar directamente os afectados:

- a) Nomes e apelidos, incluídos os doutros pasaxeiros que figuran no PNR, e número de persoas que figuran no PNR que viaxan xuntas;
- b) enderezo e datos de contacto;
- c) todos os datos sobre o pagamento, incluído o enderezo de facturación, na medida en que conteñan información que poida servir para identificar directamente o pasaxeiro a que se refire o rexistro PNR, ou calquera outra persoa;
- d) información sobre viaxeiros frecuentes;
- e) observacións xerais, na medida en que conteñan información que poida servir para identificar directamente o pasaxeiro a que se refire o rexistro, e
- f) todos os datos API sobre os pasaxeiros.

3. Ao finalizar o período de seis meses mencionado no punto 2, só se permitirá a transmisión dos datos completos cando concorran as dúas circunstancias seguintes:

- a) Que sexa necesario para os efectos establecidos no artigo 12.2.b).
- b) Que fose aprobada por unha autoridade xudicial ou pola persoa titular da Secretaría de Estado de Seguridade. Neste último caso, o responsable de protección de datos da UIP será informado da transmisión, que estará suxeita á revisión, *a posteriori*, por parte deste.

4. Os datos PNR serán suprimidos de modo permanente ao finalizar o período a que se refire o punto 1. Esta obrigación entenderase sen prexuízo daqueles casos en que se transferisen datos PNR específicos a unha autoridade competente e esta os estea utilizando no marco dun asunto concreto para efectos de previr, detectar, investigar ou axuizar delitos de terrorismo ou delitos graves, caso en que a conservación dos datos por parte da autoridade competente se rexerá pola normativa específica.

5. Os resultados do tratamento a que se refire o artigo 12.2.a) serán conservados pola UIP durante o tempo necesario para informar dun resultado positivo ás autoridades competentes e ás unidades de información sobre pasaxeiros doutros Estados membros.

Cando o resultado dun tratamento automatizado, tras un exame individual por medios non automatizados, amose un resultado negativo, poderase almacenar para evitar falsos resultados positivos posteriores, mentres os datos de base non se eliminasen segundo o punto 4.

#### Artigo 20. *Competencias da Axencia Española de Protección de Datos.*

Ademais das competencias que lle outorga a súa normativa específica, a Axencia Española de Protección de Datos, na súa condición de autoridade nacional de control de datos PNR para os efectos previstos nesta lei orgánica, exercerá as seguintes competencias:

a) Asesorar, logo de solicitude, sobre a aplicación das disposicións adoptadas en España para aplicar a Directiva (UE) 2016/681 do Parlamento Europeo e do Consello, do 27 de abril de 2016, e controlar a súa aplicación co fin de protexer os dereitos fundamentais de calquera interesado no relativo ao tratamento de datos persoais.

b) Coñecer das reclamacións presentadas contra os tratamentos realizados ao abeiro desta lei orgánica e darlles resposta nun prazo de tempo razoable.

c) Verificar a legalidade dos tratamentos, por propia iniciativa ou como consecuencia dunha reclamación, para o cal poderá realizar investigacións, inspeccións e auditorías, de acordo co disposto na súa normativa reguladora, sen prexuízo das funcións que corresponden ao Consello Xeral do Poder Xudicial como autoridade de control dos tratamentos de datos vinculados ao exercicio da función xurisdiccional.

### CAPÍTULO III

#### Réxime sancionador

##### *Sección 1.<sup>a</sup> Disposicións xerais*

#### Artigo 21. *Suxeitos responsables.*

A responsabilidade polas infraccións cometidas recaerá directamente nos suxeitos obrigados que, por acción ou omisión, realicen a conduta en que consista a infracción.

#### Artigo 22. *Responsable de tratamento e responsable de protección de datos.*

A responsabilidade do responsable de tratamento dos datos PNR e do responsable de protección de datos PNR determinarase de acordo co disposto na lexislación que traspoña a Directiva (UE) 2016/680 do Parlamento Europeo e do Consello, do 27 de abril de 2016, e, ata ese momento, polas normas que regulen no dereito español o tratamento de datos persoais por parte das autoridades competentes para fins de prevención, investigación, detección e axuizamento de infraccións penais ou de execución de sancións penais.



Artigo 23. *Regra especial.*

Para os efectos exclusivos desta lei orgánica, entenderase que os incumprimentos da obrigaón de transmisión ou remisión dos datos PNR que se produzan en relación cun mesmo voo constitúen unha única infracción.

Artigo 24. *Concurso de normas.*

1. Sempre que non constitúan infraccións á normativa xeral de protección de datos de carácter persoal, os feitos susceptibles de seren cualificados consonte dous ou máis preceptos desta ou doutra lei orgánica sancionaranse observando as seguintes regras:

- a) O precepto especial aplicarase con preferencia ao xeral.
- b) O precepto máis amplo ou complexo absorberá o que sancione as infraccións subsumidas naquel.
- c) Na falta dos criterios anteriores, aplicarase o precepto que sancione os feitos coa sanción maior.

2. No caso de que un só feito constituía dúas ou máis infraccións, ou cando unha delas sexa medio necesario para cometer a outra, a conduta será sancionada por aquela infracción á cal se lle aplique unha maior sanción.

*Sección 2.ª Infraccións*

Artigo 25. *Clasificación das infraccións.*

As infraccións tipificadas nesta lei orgánica clasifícanse en moi graves, graves e leves.

Artigo 26. *Infraccións moi graves.*

Constitúen infraccións moi graves:

- a) A falta de remisión dos datos PNR, de acordo co establecido no artigo 10.1 e 2, cando se xerese un risco grave para a seguridade cidadá, a vida ou a integridade física das persoas.
- b) A falta de remisión dos datos PNR, conforme os formatos e protocolos a que se refire o artigo 9.4, cando se xerese un risco grave para a seguridade cidadá, a vida ou a integridade física das persoas.
- c) En caso de requirimento previo, a falta de remisión dos datos PNR ou a remisión fóra do prazo concedido para o efecto, cando se xerese un risco grave para a seguridade cidadá, a vida ou a integridade física das persoas.
- d) A falta de transmisión dos datos PNR á UIP nos supostos a que se refire o artigo 10.3.

Artigo 27. *Infraccións graves.*

Constitúen infraccións graves:

- a) A falta de remisión dos datos PNR, de acordo co establecido no artigo 10.1 e 2.
- b) A falta de remisión dos datos PNR, conforme os formatos e protocolos a que se refire o artigo 9.4.
- c) A falta de adopción en tempo e forma, por parte dos suxeitos obrigados, das medidas necesarias para realizar legalmente as transmisións.
- d) En caso de requirimento previo, a falta de remisión dos datos PNR ou a remisión fóra do prazo establecido para o efecto ou sen cumprir cos requisitos técnicos e legais de transmisión.
- e) As omisións na transmisión de datos.

f) A falta de comunicación, conforme o disposto nesta lei orgánica, de calquera cambio producido previamente ou durante o traxecto, respecto ao destino onde se tivese previsto aterrar.

g) A falta de dilixencia no mantemento dos sistemas electrónicos seguros de transmisión dos datos PNR sempre que non constituía infracción consonte a normativa xeral de protección de datos de carácter persoal.

#### Artigo 28. *Infraccións leves.*

Constitúen infraccións leves:

a) O incumprimento da obrigaón de informar a UIP sobre os formatos de datos e protocolos de transmisión no prazo previsto.

b) Calquera outro incumprimento do previsto nesta lei orgánica e que non constituía infracción grave ou moi grave.

### *Sección 3.<sup>a</sup> Sancións*

#### Artigo 29. *Sancións.*

As infraccións moi graves serán sancionadas con multa de 60.001 a 300.000 euros; de 20.001 a 60.000 euros as graves, e de 3.000 a 20.000 euros as leves.

#### Artigo 30. *Gradación das sancións.*

Atendendo ao principio de proporcionalidade, graduarase a contía das sancións tendo en conta, entre outras, as seguintes circunstancias, ademais das previstas no artigo 29 da Lei 40/2015, do 1 de outubro:

a) A incidencia na seguridade pública e/ou nos dereitos á intimidade, á protección de datos, á imaxe ou á honra das persoas.

b) O beneficio económico obtido como consecuencia da comisión da infracción.

c) A natureza, gravidade e duración da infracción, tendo en conta o número de afectados e os danos ou perdas que sufrisen.

d) O grao de cooperación para pór remedio ou mitigar os posibles efectos adversos.

#### Artigo 31. *Competencia sancionadora.*

Son órganos competentes para impor as sancións:

a) A persoa titular do Ministerio do Interior, para a sanción das infraccións moi graves.

b) A persoa titular da Secretaría de Estado de Seguridade, para a sanción das infraccións graves e leves.

### *Sección 4.<sup>a</sup> Normas especiais de procedemento sancionador*

#### Artigo 32. *Medidas provisionais.*

Os gastos ocasionados pola adopción das posibles medidas provisionais serán por conta do causante dos feitos obxecto do procedemento sancionador. Estes gastos, se é o caso, serán reclamables mediante o procedemento administrativo de constrinximento cando a sanción adquiera firmeza en vía administrativa.

#### Artigo 33. *Caducidade do procedemento.*

O procedemento caducará transcorrido un ano desde a súa incoación sen que se notificase a resolución. Con todo, deberanse ter en conta no cómputo as posibles paralizacións por causas imputables ao interesado ou a suspensión que se deba acordar

pola existencia dun procedemento xudicial penal, cando concorra identidade de suxeito, feito e fundamento, ata a finalización deste.

Artigo 34. *Acceso aos datos doutras administracións públicas.*

Os órganos competentes para impor as sancións previstas nesta lei orgánica poderán acceder, no exercicio das ditas competencias, aos datos relativos aos suxeitos infractores que estean directamente relacionados coa investigación dos feitos constitutivos de infracción, coas debidas garantías de seguridade, integridade e dispoñibilidade. O acceso e o tratamento posterior dos datos realizaranse, en todo caso, de conformidade co establecido na normativa reguladora de protección de datos de carácter persoal.

Disposición adicional primeira. *Prazo para comunicar os formatos de datos e protocolos de transmisión.*

As compañías aéreas informarán a UIP do formato de datos e do protocolo de transmisión que utilizarán, no prazo de corenta días contado desde a data de publicación no «Boletín Oficial del Estado» desta lei orgánica. O formato e o protocolo deberán estar entre os previstos na Decisión de execución (UE) 2017/759 da Comisión, do 28 de abril de 2017.

Disposición adicional segunda. *Transmisión de datos PNR.*

As transmisións de datos PNR realizaranse segundo os medios de transmisión establecidos pola Secretaría de Estado de Seguridade, de acordo co disposto no artigo 9.

Disposición adicional terceira. *Réxime xurídico do acceso por parte do Centro Nacional de Intelixencia a datos PNR.*

O acceso aos datos PNR por parte do Centro Nacional de Intelixencia e o seu control realizaranse de acordo co previsto nesta lei orgánica, salvagardando, en todo caso, o carácter de materia legalmente clasificada como segredo das súas actividades e obxectivos, co fin de dar cumprimento ás misións e funcións establecidas na Lei 11/2002, do 6 de maio, reguladora do Centro Nacional de Intelixencia.

Disposición adicional cuarta. *Transmisións de datos PNR ás direccións xerais da Policía e da Garda Civil e ás autoridades competentes das comunidades autónomas que contén cun corpo de policía propio e integral.*

As transmisións de datos PNR ás direccións xerais da Policía e da Garda Civil e o seu control realizaranse de acordo co previsto nesta lei orgánica, salvagardando, en todo caso, o carácter reservado das súas investigacións e da intelixencia xerada arredor dos ditos datos en relación con delitos de terrorismo e demais delitos graves.

Igual réxime de transmisión e salvagarda das súas investigacións e intelixencia que as mencionadas no parágrafo anterior se aplicarán ás autoridades competentes das comunidades autónomas que asumisen competencias para a protección de persoas e bens e para o mantemento da seguridade cidadá e contén con corpo de policía propio.

Disposición adicional quinta. *Transmisións de datos PNR á Dirección Adxunta de Vixilancia Alfandegueira.*

As transmisións de datos PNR á Dirección Adxunta de Vixilancia Alfandegueira e o seu control faranse de acordo co previsto nesta lei orgánica, salvagardando, en todo caso, o carácter reservado dos datos con transcendencia tributaria, de acordo coa Lei 58/2003, do 17 de decembro, xeral tributaria, das súas investigacións e da intelixencia xerada arredor de tales datos en relación con delitos graves da súa competencia.

Disposición adicional sexta. *Transmisións de datos PNR a xuíces, tribunais e Ministerio Fiscal.*

As transmisións de datos PNR a xuíces, tribunais e Ministerio Fiscal faranse de acordo co previsto nesta lei orgánica, sen prexuízo da aplicación ao seu tratamento da lexislación reguladora do exercicio da potestade xurisdiccional.

En particular, as transmisións de datos PNR a xuíces e tribunais efectuaranse de acordo co previsto no artigo 14.4 desta lei orgánica.

Disposición derradeira primeira. *Título competencial.*

Esta lei orgánica dítase ao abeiro do previsto no artigo 149.1.1.<sup>a</sup> e 29.<sup>a</sup> da Constitución, que atribúen ao Estado a competencia exclusiva para a regulación das condicións básicas que garantan a igualdade de todos os españois no exercicio dos dereitos e no cumprimento dos deberes constitucionais, e sobre a seguridade pública, respectivamente.

Disposición derradeira segunda. *Preceptos que teñen carácter de lei orgánica.*

1. Teñen carácter orgánico os seguintes preceptos:
  - a) Os artigos 4 e 5.
  - b) O capítulo II.
  - c) A disposición derradeira segunda.
2. Os preceptos non incluídos no punto anterior teñen carácter de lei ordinaria.

Disposición derradeira terceira. *Incorporación de dereito da Unión Europea.*

Mediante esta lei orgánica incorpórase ao dereito español a Directiva (UE) 2016/681 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativa á utilización de datos do Rexistro de Nomes dos Pasaxeiros (PNR) para a prevención, detección, investigación e axuizamento dos delitos de terrorismo e da delincuencia grave.

Disposición derradeira cuarta. *Entrada en vigor.*

Esta lei orgánica entrará en vigor aos dous meses da súa publicación no «Boletín Oficial del Estado», agás a disposición adicional primeira, que entrará en vigor o día seguinte ao da dita publicación.

Por tanto,

Mando a todos os españois, particulares e autoridades, que cumbran e fagan cumprir esta lei orgánica.

Madrid, 16 de setembro de 2020.

FELIPE R.

O presidente do Goberno,  
PEDRO SÁNCHEZ PÉREZ-CASTEJÓN