

I

La Orden INT/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos, que viene a ser modificada por el Proyecto de Orden examinado, trae causa, como expresa su Exposición de Motivos, del artículo 12 de la Ley Orgánica 1/1992, de 21 de febrero, de Protección de la Seguridad Ciudadana, hoy día sustituido por el art. 25.1 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, así como del artículo 45 del Convenio de aplicación del Acuerdo de Schengen, de 19 de junio de 1990.

Esta Agencia, en su Informe 103/2018, sobre el Proyecto de Real Decreto por el que se establecían las obligaciones de registro documental e información de las personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor, (norma que finalmente no ha visto la luz), ya entendió, con cita del Informe de esta AEPD 203/2003, de 9 de julio de 2003, que los tratamientos de datos impuestos por el Proyecto sometido a informe a quienes ejercen actividades de hospedaje y alquiler de vehículos de motor se encontraría amparado por lo dispuesto en el artículo 6.1 c) del RGPD, en cuanto que constituye una obligación legal impuesta a sus destinatarios.

El art. 6.3 RGPD, al referirse a esta base jurídica añade que ésta deberá ser establecida bien por el derecho de la Unión, bien por el derecho del Estado miembro que se aplique al responsable del tratamiento, y que dicha base jurídica ***podrá*** *contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento*, citando alguna de las disposiciones específicas que el legislador estatal o europeo puede adaptar en estos casos.

La norma de la que se deriva esta obligación legal (art. 25.1 de la Ley Orgánica 4/2015, de 30 de marzo) no contiene estas disposiciones específicas permitidas por el RGPD para adaptar la aplicación del RGPD a dicho tratamiento. El Tribunal Constitucional ha tenido ocasión de examinar los requisitos para que las leyes que establecen tratamientos de datos personales, en cuanto que restricciones al derecho fundamental a la protección de datos personales del interesado, puedan considerarse conformes a la Constitución. Así, dicha doctrina constitucional puede resumirse en la sentencia del Tribunal Constitucional (STC) 76/2019, de 22 de mayo, que aborda tanto las características y el contenido que ha de tener la normativa que pretenda establecer una injerencia en ese derecho fundamental.

(...) Por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas ora incida directamente sobre su desarrollo (artículo 81.1 CE), ora limite o condicione su ejercicio (artículo 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril, FJ 4). (...) Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, esa norma legal «ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica», esto es, «ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención» (STC 49/1999, FJ 4). En otras palabras, «no sólo excluye apoderamientos a favor de las normas reglamentarias [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites» (STC 292/2000, FJ 15).

Y por otra parte,

el Reglamento general de protección de datos establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales. En cambio, no establece por sí mismo el régimen jurídico aplicable a los tratamientos de datos personales especiales, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión.

En consecuencia, cuando los tratamientos son de datos personales que no pertenecen a categorías especiales cabe considerar que el RGPD contiene las *garantías mínimas, comunes o generales* para el tratamiento de dichos datos; lo que no sería el caso cuando los tratamientos fuesen de categorías especiales de datos. No parece resultar de la normativa sometida a informe el tratamiento de categorías especiales de datos personales, por lo que la confluencia de la ley 40/2015 y su contenido con el RGPD determina que este contenga las reglas mínimas comunes o generales de estos tratamientos. Nada impediría sin embargo que el legislador orgánico en una modificación posterior de dicha norma pudiera adaptar, lo que sería recomendable, el tratamiento de datos personales previsto en el artículo 25.1 de dicha ley con normas o disposiciones más específicas conforme permite el art. 6.3 RGPD ya citado.

II

El artículo único del proyecto de Orden sometido informe modifica el apartado segundo de la Orden INT/1922/2003 para hacer posible la recogida de la firma en el libro registro de entrada en soporte digital, adaptando las previsiones del formato de dicho libro registro cuando se lleve en formato digital, o el plazo de conservación de dichos libros registro, que, cuando la información se conserve por medios digitales, se computa desde la fecha de grabación.

Respecto del plazo de conservación, de tres años, tal y como se mencionó en el ya citado informe 103/2018, se considera conforme con el principio de minimización de datos (art. 5.1.c) RGPD), y no se presentan objeciones al resto de las modificaciones establecidas en dicho artículo único.

Con una excepción, y es que no resulta ni de la modificación llevada a cabo por el proyecto de Orden ni de la regulación existente en la Orden INT/1922/2003 el que el interesado cuyos datos se recogen y tratan pueda tener copia del documento cuya firma se le exige. En opinión de esta AEPD, el derecho de información del interesado de quien se requieren datos personales necesita no sólo que este pueda conocer la información que deba facilitársele conforme al art. 13 RGPD, sino que este artículo del RGPD establece expresamente que dicha información ha de serle “facilitada”, lo que implica, cuando menos, la posibilidad de que el interesado pueda disponer, y llevar consigo, un ejemplar de lo que se le ofrece a firmar. Y ello ya se proceda a la firma en papel o en forma digital, como previene el Proyecto de Orden. Nada en esta se menciona de tal posibilidad.

En conclusión, no puede corroborarse una interpretación de la norma que determine que dicha hoja a firmar por el interesado sea una hoja única, firmada en papel o de manera digital, sin la posibilidad de que este interesado pueda disponer para sí de dicha información y llevarla consigo si lo considera oportuno. En consecuencia, se sugiere que en el proyecto se haga mención bien de que dichas hojas de libro registro serán duplicadas de manera que el interesado pueda hacerse sido considera oportuno con un duplicado de lo que firma, que incluirá la información efectos de la normativa de protección de datos; bien disponer que el interesado podrá obtener una copia (fotocopia o similar) o bien una copia del documento que ha firmado digitalmente.

III

En cuanto al modelo de Anexo, cabe mencionar lo siguiente:

En primer lugar, si bien se hace referencia en la Exposición de Motivos del Proyecto a que el modelo de Anexo de la Orden INT/1922/2003 se actualiza teniendo en cuenta las novedades de la normativa de protección de datos de carácter personal, no se hace ninguna referencia en la parte dispositiva del Proyecto a la sustitución de dicho Anexo por el nuevo Anexo que se acompaña al Proyecto, por lo que debería hacerse referencia a dicha sustitución específicamente.

En segundo lugar, la única diferencia que se aprecia entre el Anexo de la Orden INT/1922/2003 y el presentado con el Proyecto consiste en la sustitución de la referencia a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) (y a la Ley Orgánica 1/1992, de 21 de febrero, de seguridad ciudadana) por una referencia a (i) la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de

los derechos digitales, (LOPDGDD), (ii) en lo que resulte de aplicación, a la [ley] relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, y (iii) a la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana.

Los datos personales de los interesados (los huéspedes) se han de plasmar en dicho Anexo, y son los que se recogen al principio del mismo (número de documento de identidad; tipo de documento; fecha de expedición del documento; primer apellido; segundo apellido; nombre; sexo; fecha de nacimiento; país de nacionalidad, y fecha de entrada) son obtenidos de dichos interesados por el responsable del tratamiento (el hostelero).

El art. 13.1 y el art. 13.2 RGPD establece toda la información que ha de facilitar el responsable al interesado cuando los datos se obtienen de este:

Información que deberá facilitarse cuando los datos personales se obtengan del interesado

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, **en el momento en que estos se obtengan**, le facilitará toda la información indicada a continuación:

- a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
- b) los datos de contacto del delegado de protección de datos, en su caso;
- c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
- d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
- e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
- f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

- a) *el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;*
- b) *la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;*
- c) *cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;*
- d) *el derecho a presentar una reclamación ante una autoridad de control;*
- e) *si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;*
- f) *la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.*

Igualmente, el apartado 4 del art. 12 RGPD dispone que cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

Por ello, y salvo en los casos en que ya el interesado ya dispusiera de toda esa información -cuestión que corresponderá probar al responsable- el responsable (en este caso el hostelero) habrá de proporcionar al interesado toda la información a que se refieren los artículos 13.1 y 13.2 RGPD, y el momento para ello es el de la lectura y firma por el huésped del Modelo de parte de entrada de viajeros, que es cuando dichos datos se recogen del interesado. En conclusión, el Modelo deberá contener toda la información a que se refiere dichos preceptos citados (art. 13 RGPD) que se correspondan con un tratamiento cuya base jurídica es el cumplimiento de una obligación legal (no será por tanto aplicable el apartado d) del art. 13.1 RGPD, por ejemplo).

No obstante lo anterior, el art. 11.1 LOPDGDD establece en estos casos el responsable puede proporcionar a los interesados (afectados) dicha información facilitándoles la *información básica* a la que se refiere el apartado 2 de dicho artículo e indicándole una *dirección electrónica* u otro medio que

permita acceder de forma sencilla e inmediata a la *restante* información. Esto es, lo que se denomina información *por capas*. La información básica deberá contener, *al menos*: a) La identidad del responsable del tratamiento y de su representante, en su caso. b) La finalidad del tratamiento, y c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Ello habrá de ser tenido en cuenta por el redactor del Proyecto de Orden respecto del Anexo, para determinar cómo se recoge en él la información necesaria a proporcionar al interesado de quien se toman sus datos.

IV

Cabe referirse al tratamiento posterior de datos por parte de las Fuerzas y Cuerpos de Seguridad del Estado (FyCSE), que es el fin último de dicha norma.

El ya citado Informe de esta AEPD 103/2018, sobre el Proyecto de Real Decreto por el que se establecían las obligaciones de registro documental e información de las personas físicas o jurídicas que ejercen actividades de hospedaje y alquiler de vehículos a motor, (norma que -se reitera- no ha visto la luz), recordó que *[l]a existencia de una base legal adecuada para el tratamiento no impide, sin embargo, que sea necesario analizar si el tratamiento y comunicación de los datos a los que se refiere el Proyecto cumple adecuadamente con los principios de protección de datos consagrados por el artículo 5.1 del Reglamento general de protección de datos. En este sentido, debe recordarse en particular que el artículo 5.1 c) consagra el principio de minimización en el tratamiento de datos personales, al disponer que los datos deberán ser “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”.*

Además, cualquier tratamiento de datos personales ha de cumplir con el principio de proporcionalidad en cuanto que tal tratamiento constituye una injerencia en un derecho fundamental. En la sentencia del Tribunal de Justicia de la UE (STJUE) de 16 de julio de 2020, C-311/18, Schrems 2, (y se reitera posteriormente en las sentencias de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, y en la de la misma fecha 6 de octubre de 2020 (C-623/17), Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros) se establece que:

*176 Finalmente, para cumplir el requisito de **proporcionalidad** según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer **reglas claras y precisas** que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias*

*mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de **garantías suficientes** que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada].*

Recuerda el tan reiterado Informe 103/2018 de esta AEPD que *[e]n relación con el principio de minimización de datos debe tenerse en cuenta la doctrina sentada por el Tribunal de Justicia de la Unión Europea a partir de las sentencias de 8 de abril de 2014 (asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland Ltd.) y 21 de diciembre de 2016 (asuntos acumulados C-203/15 y C-698/15, Tele2 Sverige AB), en que se viene a declarar contrario al derecho de la Unión el tratamiento masivo e indiscriminado de datos de tráfico en comunicaciones electrónicas al considerarse el mismo una intromisión en los derechos fundamentales a la intimidad y a la protección de datos personales, consagrados en los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea.*

Citado todo lo anterior cabe recordar la necesidad de que todo tratamiento de datos personales cumpla el principio de proporcionalidad, y que establezca regla claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de un uso indebido.

Los apartados Tercero y Cuarto de la Orden INT/1922/2003, de 3 de julio, sobre libros-registro y partes de entrada de viajeros en establecimientos de hostelería y otros análogos, establecen que los establecimientos comprendidos en el ámbito de aplicación de la Orden deberán comunicar a las dependencias policiales la información contenida en las hojas-registro dentro de las veinticuatro horas siguientes al comienzo del alojamiento de cada viajero. De ello resulta que la norma prevé que los destinatarios de los datos serán las FyCSE, pero no existe en la actualidad una determinación clara de la finalidad de dicho tratamiento por dichas FyCSE. El Proyecto de Real Decreto informado en el Informe 103/2018 restringía dicha finalidad a “las competencias de prevención e investigación del delito que tengan asignadas”, y que “[e]l tratamiento de los datos de carácter personal derivados de la ejecución de este real decreto se llevará a cabo conforme a la normativa de protección de datos de carácter personal por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o

de ejecución de sanciones penales”. Se restringe, en definitiva, los tratamientos por las FyCSE a la investigación en materia penal; pero en la norma actual dicha restricción no aparece, ni la misma se predica indubitadamente de la ley orgánica 4/2015. El borrador de Anexo presentado a Informe tampoco lo acaba de concretar, porque a la vez que la cita a las disposiciones de la LOPDGDD añade que dichos datos se tratarán *“en lo que resulte de aplicación”*, conforme a la normativa *“relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales”*, así como añade, conforme a la *“Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana artículo 25.1”*. No existe por lo tanto una concreción de cuáles son las finalidades concretas para que las FyCSE podrán utilizar dichos datos personales, o de qué forma lo usarán, o si los cruzarán con otras bases de datos, o cuáles, o con qué **“objetivos”** precisos -conforme requiere el art. 8 de la Directiva 2016/680,- concepto este (el de “objetivo”) distinto y adicional a las “finalidades” de los tratamientos, puesto que estas últimas, en el ámbito de la Directiva 2016/680, tan sólo pueden ser la prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. El art. 8 de la Directiva 2016/680 establece que *el Derecho del Estado miembro que regule el tratamiento dentro del ámbito de aplicación de la presente Directiva, deberá indicar al menos los **objetivos** del tratamiento, los datos personales que vayan a ser objeto del mismo y las **finalidades** del tratamiento*. Como es sabido, esta Directiva no ha sido aun traspuesta al derecho español, estableciendo la Disposición transitoria cuarta de la LOPDGDD que los tratamientos sometidos a 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, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.

En definitiva, esta AEPD considera que el tratamiento de datos personales por las FyCSE de los datos obtenidos en virtud de las fichas de estancia debería de estar definido de manera más concreta, estableciéndose claramente los “objetivos”, y la finalidad de dicho tratamiento, delimitando que estos serán exclusivamente para fines de investigación de infracciones penales, y estableciendo reglas claras y precisas, así como las garantías suficientes, para que los interesados puedan conocer los tratamientos posibles que la norma prevé sobre sus datos y permitan proteger de manera eficaz sus datos de carácter personal.