

CNS 7/2019

Dictamen en relación con la consulta formulada por una AFA de una escuela pública en lo referente a la adaptación de sus actuaciones a la normativa de protección de datos.

Se presenta ante la Autoridad Catalana de Protección de Datos un escrito de una AFA de una escuela pública, en el que se formula una consulta sobre cómo adaptar sus actuaciones a la normativa de protección de datos.

La consulta se acompaña de un documento llamado “Evaluación de impacto relativo a la protección de datos”.

Analizada la petición, y la documentación que le acompaña, y visto el informe de la Asesoría Jurídica, se dictamina lo siguiente

(...)

II

AFA, solicita el asesoramiento de la APDCAT para adaptarse a la normativa de protección de datos y aporta con la solicitud un documento que se denomina “Evaluación de impacto relativo a la protección de datos”.

AFA, para alcanzar sus objetivos, trata información de sus socios, alumnos, colaboradores, trabajadores y voluntarios. Estos datos, en la medida en que se refieran a personas físicas identificables, tienen consideración de datos de carácter personal y, por tanto, se encuentran protegidos por la normativa de protección de datos de carácter personal.

En consecuencia, cualquier tratamiento de estos datos, incluyendo la recogida o cualquier utilización o tratamiento posterior que se realice, queda sometido a los principios y garantías que se contienen en la normativa de protección de datos. En concreto, en el Reglamento (UE) 2016/679, del Parlamento y del Consejo Europeo, de 27 de abril de 2016, General de Protección de Datos (en adelante RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantizada de los Derechos Digitales (en adelante LOPDGDD).

Dicho esto, y en lo que se refiere al documento llamado “evaluación de impacto relativo a la protección de datos” que se adjunta a la consulta, la normativa de protección de datos, dispone que con carácter previo al inicio del tratamiento, el responsable debe realizar una evaluación del impacto en la protección de datos (en adelante AIPD) cuando este tratamiento, por su naturaleza, alcance, contexto o finalidades, suponga un alto riesgo por los derechos y libertades de las personas físicas, especialmente cuando se utilicen nuevas tecnologías (considerando 76 y artículo 35 del RGPD).

Así, por un lado, el artículo 35.3 del RGPD establece que, entre otros supuestos, es necesario realizar una evaluación de impacto relativa a la protección de datos en los siguientes supuestos:

- a) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas basada en un tratamiento automatizado, como la elaboración de perfiles, sobre cuya base se toman decisiones que producen efectos jurídicos para las personas físicas o que les afectan significativamente de modo similar.
- b) Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a las que se refiere el artículo 10.
- c) Observación sistemática a gran escala de una zona de acceso público.

Para la delimitación de la que hay que entender por “tratamiento a gran escala”, el Grupo del artículo 29, en su dictamen sobre la designación de delegados de protección de datos, considera que debe tenerse en cuenta lo siguiente:

- El número de interesados afectados, ya sea en términos absolutos o como proporción de una determinada población.
- El volumen y la variedad de datos tratados.
- La duración o permanencia de la actividad de tratamiento.
- La extensión geográfica de la actividad de tratamiento.

Además, la LOPDGDD (DA 17^a) ha previsto expresamente que será necesario realizar una evaluación de impacto que determine los riesgos derivados de tratamientos con fines de investigación en salud pública y, en particular biomédica, que deberá evaluar específicamente los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

Por otra parte, más allá de los supuestos previstos directamente en el RGPD y en el LOPDGDD, y siguiendo las Directrices sobre la evaluación de impacto relativa a la protección de datos (AIPD) y para determinar si el tratamiento comporta probablemente un alto riesgo a efectos del Reglamento (UE) 2016/679, adoptadas por el Grupo de Trabajo del Artículo 29 el 4 de abril de 2017 (en adelante, WP 248) esta Autoridad, en los tratamientos que no sean transfronterizos, considera necesario realizar una evaluación del impacto relativa a la protección de datos en los tratamientos que se quieran llevar a cabo que cumplan dos o más de las siguientes circunstancias:

- Evaluación o “puntuación” de personas, incluida la elaboración de perfiles y la predicción de conductas o comportamientos.
- Toma de decisiones automatizada con efecto jurídico o similar significativo.
- Observación sistemática.
- Datos sensibles o datos muy personales (categorías especiales de datos del artículo 9 RGPD o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 RGPD).
- Tratamientos de datos a gran escala.
- Asociación o combinación de conjunto de datos que pueden exceder las expectativas razonables de las personas interesadas.
- Datos relativos a sujetos vulnerables (menores, empleados, personas discapacitadas, personas mayores, solicitantes de asilo o refugiados, etc.).
- Utilización innovadora o aplicación de nuevas soluciones tecnológicas o organizativas.
- Cuando el tratamiento impide a las personas afectadas ejercer un derecho, utilizar un servicio o ejecutar un contrato.

La evaluación de impacto relativa a la protección de datos, en principio no debe referirse a todas las actividades de llevada a cabo un responsable o un encargado del tratamiento, sino sólo a aquellos en los que concurran las circunstancias mencionadas.

Teniendo en cuenta todo esto, esta Autoridad considera que los tratamientos descritos por la AFA no se incluyen en ninguno de los supuestos previstos actualmente en la normativa de protección de datos ni en las circunstancias establecidas por esta Autoridad en que hay que realizar, con carácter previo en su tratamiento, una evaluación del impacto. Por tanto, en este caso concreto, la AIPD no sería obligatoria, aunque nada impide hacerlo con carácter voluntario.

En cualquier caso, el documento que aporta la asociación y que se denomina "Evaluación de impacto relativo a la protección de datos" no incluye el contenido mínimo que establece el artículo 35.7 del RGPD y, por tanto, no puede considerarse una AIPD. Esto no quita que esta Autoridad valore el esfuerzo realizado por la AFA por cumplir con la normativa de protección de datos.

A título informativo, puede consultar las Directrices del Grupo de trabajo del artículo 29 sobre la evaluación de impacto relativa a la protección de datos (AIPD) y para determinar si el tratamiento comporta probablemente un alto riesgo a efectos del Reglamento (UE) 2016/679 (WP 248), asumidas por el Comité Europeo de Protección de datos en su reunión de 25 de mayo de 2018, y la Guía práctica de la APDCAT sobre la evaluación de impacto relativa a la protección de datos en el RGPD (<http://apdcata.gencat.cat/web/.content/03-documentación/>).

III

Dicho esto, para adecuarse a la normativa en materia de protección de datos deberá cumplir con el conjunto de las obligaciones reguladas en el Reglamento general de protección de datos. En este informe, con el objetivo de darle el apoyo necesario para que pueda adaptarse, le ofrecemos información general sobre algunas de las obligaciones que debe tener en cuenta a la hora de tratar los datos. No obstante, el cumplimiento responsable de lo establecido en el Reglamento requiere un análisis esmerado de todas las obligaciones previstas en el RGPD teniendo en cuenta las circunstancias concretas de cada uno de los tratamientos que se lleven a cabo.

La AFA debe cumplir lo que establece el RGPD. Por tanto, el tratamiento de los datos siempre debe llevarse a cabo respetando los principios del RGPD (art. 5 RGPD) y de modo que se pueda demostrar que el cumplimiento (responsabilidad proactiva y demostrable).

Los datos personales deben ser tratados según los principios enunciados en el artículo 5 del RGPD. Así, los datos deben ser:

- a. Tratadas de forma lícita, leal y transparente en relación con el interesado (licitud, lealtad y transparencia).
- b. Recogidas con finalidades determinadas, explícitas y legítimas y posteriormente no deben tratarse de forma incompatible con estas finalidades.
- c. Adecuadas, pertinentes y limitadas a lo necesario en relación con las finalidades para las que se tratan (minimización de datos).
- d. Exactas y, en su caso, deben actualizarse.
- e. Conservadas de forma que permitan identificar a los interesados durante un período no superior al necesario para las finalidades del tratamiento de datos personales ("limitación del plazo de conservación").
- f. Tratadas de forma que se garantice una seguridad adecuada ("integridad y confidencialidad").

De acuerdo con el principio de licitud, el responsable del tratamiento sólo puede tratarlas si concurre alguna de las bases jurídicas establecidas en el artículo 6 del RGPD. En concreto:

- a. Que disponga del consentimiento de la persona afectada para una o varias finalidades específicas.
- b. Que sea necesario para ejecutar un contrato en el que el interesado es parte o por aplicar medidas precontractuales a petición del interesado.
- c. Que sea necesario para cumplir una obligación legal del responsable del tratamiento.
- d. Que sea necesario para proteger intereses vitales del interesado o de otra persona física.
- e. Que sea necesario para cumplir una misión realizada en interés público o en el ejercicio de poderes públicos otorgados al responsable del tratamiento.
- f. Que sea necesario para satisfacer intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que no prevalezcan intereses o derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un menor.

En el caso de tratamientos necesarios para el cumplimiento de una obligación legal (letra c) o de una misión realizada en interés público o en el ejercicio de poderes públicos (letra e), la base del tratamiento debe estar prevista por el derecho de la Unión o por el derecho del estado miembro, que en nuestro caso debe ser una norma con rango de ley.

Además, el tratamiento de categorías especiales de datos personales (artículo 9 RGPD) está permitido cuando: a. El tratamiento se efectúa con el consentimiento explícito del interesado, salvo que el derecho de la Unión o del Estado miembro no lo permita. b. El tratamiento será necesario para cumplir obligaciones o ejercer derechos en el ámbito laboral, si así lo autoriza el derecho de la Unión o del Estado miembro. c. El tratamiento es necesario para proteger intereses vitales del interesado o de un

- tercero, si no tiene capacidad para consentir con ellos.
- d. El tratamiento se realiza en el ámbito de las actividades legítimas de una entidad sin ánimo de lucro con finalidad política, filosófica, religiosa o sindical y se refiere a los miembros actuales o antiguos de la entidad.
- e. El tratamiento se refiere a datos que el interesado ha realizado manifiestamente públicas.
- f. El tratamiento será necesario para formular, ejercer o defender reclamaciones o cuando los tribunales actúen en el ejercicio de su función judicial.
- g. El tratamiento es necesario por razones de interés público esencial.
- h. El tratamiento es necesario para fines de medicina preventiva y del trabajo, diagnóstico médico y prestación y gestión de asistencia sanitaria, sobre la base del derecho de la Unión o de un estado miembro o siempre que el tratamiento lo realice un profesional sanitario sujeto a secreto profesional u otra persona sujeta al deber de confidencialidad.
- i. El tratamiento es necesario por razones de salud pública sobre la base del derecho de la Unión o de un Estado miembro.
- j. El tratamiento es necesario para fines de archivo en interés público, de investigación científica o histórica o fines estadísticos en base al derecho de la Unión o de un Estado miembro.

Los datos personales relativos a condenas e infracciones penales sólo pueden tratarse bajo la supervisión de las autoridades públicas o cuando lo autoriza el derecho de la Unión o del Estado miembro, que debe establecer garantías adecuadas para los derechos y libertades de los interesados (artículo 10 RGPD).

Cuando la base jurídica que legitima el tratamiento es el consentimiento, que debe ser libre, específico e inequívoco, la persona interesada tiene derecho a retirarlo o revocarlo en

cualquier momento. La retirada o revocación del consentimiento no tendrá efectos retroactivos. Por tanto, no afecta a la licitud del tratamiento fundamentada en el consentimiento previo a la retirada. Por otra parte, retirar el consentimiento debe ser tan sencillo como prestarlo.

IV

Aparte del cumplimiento de los principios, el RGPD prevé una serie de obligaciones que debe cumplir el responsable del tratamiento.

a) Llevar un Registro de actividades de tratamiento

El RGPD ha suprimido la obligación de notificar los archivos a la autoridad de control en materia de protección de datos para su registro. No obstante, contempla nuevas obligaciones de documentación del tratamiento para los responsables o encargados del tratamiento, en concreto, la necesidad de llevar un registro de las actividades de tratamiento. Sólo se exceptúan de esta obligación los responsables o encargados del tratamiento que cuenten con menos de 250 trabajadores. Sin embargo, esta excepción no es de aplicación si se da alguna de las siguientes circunstancias (art. 30.5 RGPD): si es probable que exista un riesgo para los derechos y libertades de los sujetos afectados; si el tratamiento no es ocasional; o si el tratamiento incluye categorías especiales de datos o relativas a infracciones y condenas penales. En cualquier caso, este registro contendrá, respecto de cada actividad, la información establecida en el artículo 30 del RGPD.

La APDCAT ha desarrollado una aplicación sencilla para llevar el registro de actividades del tratamiento para que los responsables y los encargados del tratamiento (http://apdcatt.gencat.cat/ca/documentacio/RGPD/altres_documents_dinteres).

b) Informar a las personas interesadas

En el momento de recoger la información, es necesario informar a las personas interesadas sobre las condiciones en que se lleva a cabo el tratamiento de los datos personales (artículo 13 RGPD y 11 de la LOPDDDD), especialmente, sobre la finalidad o las finalidades para las cuales se tratarán los datos.

La información debe hacer referencia a:

- La identidad y datos de contacto del responsable y, en su caso, de su representante.
- Los datos de contacto del delegado de protección de datos.
- Las finalidades y la base jurídica del tratamiento.
- Los destinatarios o categorías de destinatarios de los datos.
- La intención de transferir los datos a un tercer país o a una organización internacional y la base para ello, si procede.
- El plazo durante el cual se conservarán los datos o criterios para determinar lo.
- El derecho a solicitar el acceso a los datos, rectificarlos o suprimirlos, limitar su tratamiento, oponerse a ellos y solicitar su portabilidad.
- El derecho a retirar en cualquier momento el consentimiento que se ha prestado.
- Si la comunicación de datos es un requisito legal o contractual o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos y está informado de las consecuencias de no hacerlo.

- El derecho a presentar una reclamación ante una autoridad de control, o, en su caso, ante el Delegado de protección de datos.
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y la información sobre la lógica aplicada y sus consecuencias.

Esta información debe darse de forma accesible y fácil de entender, con lenguaje sencillo y claro, especialmente cuando la información se dirige a un menor, indicando para que se recojan, utilicen o traten estos datos, tal y cómo exige el RGPD. Al respecto, puede ser de interés consultar la Guía para el cumplimiento del deber de información en el RGPD (http://apdcat.gencat.cat/ca/documentacio/guies_basiques).

El LOPDGDD ha previsto la posibilidad de utilizar un mecanismo de doble capa para dar cumplimiento a las obligaciones de información, de tal modo que se facilite la información básica que sea pertinente, en función de si los datos se han obtenido de la propia persona interesada o de un tercero, con la posibilidad de remitir a una dirección de correo electrónico u otro medio que permita a la persona interesada acceder al resto de información prevista en el RGPD.

c) Encargos de tratamiento a terceras personas o entidades

En caso de tratar con terceros que presten servicios en nombre de la AFA y que traten datos personales de los socios, como por ejemplo, las actividades extraescolares, o gestionen la página web o la actividad administrativa, se tendrán que firmar los correspondientes contratos de encargados del tratamiento.

El RGPD amplía el contenido mínimo del contrato de encargo de tratamiento (artículo 28.3 RGPD y artículo 33 LOPDGDD). Entre otros aspectos, el contrato debe prever los siguientes puntos adicionales respecto del contenido que ya establecía la LOPD: el objeto y la duración del encargo; la naturaleza del tratamiento; el tipo de datos personales; las categorías de personas interesadas; las obligaciones y derechos del responsable; la previsión de que las personas que deben tratar los datos se comprometen a mantener la confidencialidad; la asistencia del encargado al responsable por atender las solicitudes de ejercicio de derechos; la supresión o devolución de los datos al finalizar el encargo; la obligación de poner a disposición del responsable toda la información necesaria para demostrar que cumple las obligaciones del encargado del tratamiento y para permitir y contribuir a que el responsable u otro auditor autorizado por el responsable efectúe auditorías e inspecciones

Al respecto, puede ser de interés consultar la Guía del encargado del tratamiento (http://apdcat.gencat.cat/ca/documentacio/guies_basiques/).

Ahora bien, si mantiene algún contrato o acuerdo de encargo del tratamiento firmado antes de 25 de mayo de 2018 debe saber que de acuerdo con la Disposición transitoria quinta de la LOPDGDD, éstos mantienen su vigencia hasta la fecha de vencimiento señalada en los mismos. Cuando se trate de encargos con duración indefinida, mantienen la vigencia hasta el 25 de mayo de 2022. En cualquier caso, durante la vigencia del contrato o acuerdo, cualquiera de las partes puede exigir a la otra la modificación del contrato para adaptarse a lo establecido en el artículo 28 del RGPD.

d) Delegado de protección de datos

Como novedad, el RGPD introduce la figura del delegado de protección de datos, que puede formar parte de la plantilla del responsable o encargado o bien actuar en el marco de un

contrato de servicios. Hay que designar a un delegado de protección de datos en los siguientes casos: - Cuando el tratamiento lo lleva a cabo una autoridad u organismo público (salvo juzgados y tribunales). En este caso, podrá designarse un único delegado de protección de datos para varias de estas autoridades u organismos.

- Cuando el tratamiento requiere la observación habitual y sistemática de interesados en gran escala.
- Cuando el tratamiento tiene por objeto categorías especiales de datos personales o datos relativos a condenas o infracciones penales.

Dados los tratamientos que se describen en la consulta, no parece que la AFA deba designar uno de forma obligatoria. Sin embargo, nada impide que se pueda designar de forma voluntaria.

Una vez designado el delegado, las entidades incluidas en el ámbito de actuación de la APDCAT deben comunicar esta designación a la Autoridad Catalana de Protección de Datos. Asimismo, es necesario mantener actualizados los datos comunicados.

A través de la sede electrónica de la Autoridad <https://seu.apd.cat/ca/tramits/DPD> puede acceder a los trámites para consultar los DPD designados o bien comunicar la designación del DPD.

e) Medidas de seguridad

También es necesario adoptar las medidas técnicas y organizativas adecuadas al riesgo que comporta el tratamiento de los datos, para garantizar el cumplimiento de la normativa y proteger los derechos de los interesados.

El RGPD no establece ningún listado basado en los niveles de seguridad básico, medio y alto, como preveía el RLOPD, sino que deja a criterio del responsable y del encargado, previo análisis de los riesgos, determinar qué medidas de seguridad se tendrán que implementar en cada supuesto.

Desde el punto de vista de la seguridad de la información un análisis de riesgos requiere identificar las amenazas (por ejemplo, acceso no autorizado a los datos personales), valorar cuál es la probabilidad de que se produzca y el impacto que tendría en las personas afectadas .

El tipo de riesgo y, en definitiva, su probabilidad y gravedad, varía según los tipos de tratamiento, la naturaleza de los datos que se tratan, el número de personas interesadas afectadas, la cantidad y variedad de tratamientos, las tecnologías utilizadas etc.

En caso de tratamientos de poca complejidad, este análisis puede ser el resultado de una reflexión documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de las personas interesadas. Esta reflexión debe analizar el contexto en el que se lleva a cabo el tratamiento (medios, instalaciones, usuarios etc.) y debe dar respuesta a cuestiones como el tipo de datos que tratan (categorías especiales de datos, de lectivos vulnerables, de una gran cantidad de personas, que permiten la elaboración de perfiles), si la revelación, alteración o pérdida de los datos puede tener consecuencias importantes para las personas afectadas, si se tratan los datos fuera de los equipos o instalaciones del responsable, si tienen acceso a los datos terceras personas que prestan servicios por cuenta del responsable, y se utilizan tecnologías especialmente invasivas para la privacidad, (geolocalización, videovigilancia, internet de las cosas etc.).

Por tanto, es muy importante que si no se utiliza una metodología estándar, fácilmente auditable y objetivable, se documenten detalladamente las cuestiones que se han tenido en cuenta a la hora de determinar el nivel de riesgo existente y concretar las medidas de seguridad que es necesario aplicar. Esto servirá para cumplir con el principio de responsabilidad proactiva.

Ahora bien, esto no quiere decir que las medidas que aplicaba siguiendo el RLOPD, no sean correctas. Quizás son las adecuadas, pero es necesario, en todo caso, realizar el análisis de riesgos para determinar si las medidas implementadas son suficientes o si hay alguna carencia. En cualquier caso, la selección de las medidas de seguridad debe garantizar un nivel de protección adecuado al riesgo.

V

Por último, a título informativo, la APDCAT, dispone de un catálogo de recursos para hacer más sencillo el cumplimiento de la normativa.

Así, tiene a su disposición un conjunto de normativa de ámbito autonómico, estatal e internacional en materia de protección de datos y otros documentos y herramientas de interés como las guías del APDCAT y las directrices del Grupo de Trabajo del Artículo 29, además de otras disposiciones adoptadas por la APDCAT (instrucciones, recomendaciones y otras disposiciones). Esta información la tiene a su disposición en la web: <http://apdc.cat/gencat.cat/ca/autoritat/normativa>

Informarse de que, a través de la sede electrónica de la Autoridad <https://seu.apd.cat>, puede acceder al resto de información, servicios y trámites que la Autoridad pone a su disposición, entre otros:

1.-Notificar las violaciones de seguridad de los datos personales: esta notificación debe formalizarse mediante el [formulario de notificación](#). Una vez generado el documento en formato pdf, con la notificación firmada electrónicamente, debe enviarse, junto con la documentación que en su caso se adjunte. Si está dado de alta en EACAT debe presentar el formulario mediante el envío genérico de esta plataforma; si no, debe presentarlo a través de [E TRAM](#)

2.-Transferencias internacionales: en este apartado la AFA puede tramitar los siguientes expedientes: autorización de transferencias internacionales de datos y/o comunicación de transferencias internacionales de datos. La solicitud debe formalizarse mediante el [formulario de alta](#). Una vez generado un documento en formato pdf con la solicitud firmada electrónicamente, puede enviarlo, junto con la documentación adjunta a través de [ETRAM](#)

3.-Solicitar un dictamen: a través del/a presidente/a de la AFA se puede pedir un dictamen a la Autoridad respecto de un tema concreto. La solicitud debe formalizarse a través de la sede electrónica.

4.-Plantear una consulta previa: El responsable del tratamiento debe realizar una consulta previa a la Autoridad Catalana de Protección de Datos con carácter previo al inicio del tratamiento, entre otros supuestos, cuando se haya elaborado una evaluación de impacto sobre la protección de datos de la que resulte que existe un alto riesgo si el responsable no toma medidas para mitigarlo. La solicitud debe [formalizarse](#) mediante el [formulario de alta](#).

Además, dispone de un servicio de consultoría personalizado para apoyar continuamente todos los proyectos de adecuación a la normativa de protección de datos personales que

realice. Para solicitar el servicio de consultoría, debe dirigir su petición por correo electrónico a: serveideconsultoria.apdcat@gencat.cat.

Todo ello sin perjuicio de que solicite otros servicios que pone a disposición la APDCAT como el servicio de atención al público al que puede dirigirse para solicitar información o consultar dudas en relación con la aplicación de la legislación de protección de datos de carácter personal, o pedir información de los cursos, conferencias, jornadas, seminarios y otras actividades formativas y divulgativas que organiza la Autoridad o en los que participa. Puede contactar con este servicio por correo electrónico: atenciopublic.apdcat@gencat.cat.

De acuerdo con las consideraciones hechas en este dictamen en relación con la consulta planteada, se hacen las siguientes,

Conclusiones

La Autoridad valora el esfuerzo por parte de la AFA por adecuarse a la normativa de protección de datos, pero considera que el documento que aporta la asociación y que llama "Evaluación de impacto relativo a la protección de datos" no incluye el contenido mínimo que establece el artículo 35.7 del RGPD. En cualquier caso, no se trata de un documento obligatorio para los tratamientos descritos en la consulta.

La AFA para adecuarse a la normativa de protección de datos debe cumplir todos los principios y obligaciones a que se refiere en términos generales este informe y cualquier otra de las establecidas en el Reglamento (UE) 2016/679, del Parlamento y del Consejo Europeo, de 27 de abril de 2016, General de Protección de Datos y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantizada de los Derechos Digitales.

Barcelona, 20 de febrero de 2019