AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

# EL NUEVO RGPD Y SU IMPACTO SOBRE LA ACTIVIDAD DE LAS ADMINISTRACIONES LOCALES

Las Administraciones Públicas (AAPP), y dentro de ellas las Administraciones Locales (AALL), actúan como responsables y encargados de tratamientos de datos personales en el desarrollo de muchas de sus actividades. Consecuentemente, se van a ver afectadas por las previsiones del nuevo Reglamento General de Protección de Datos (RGPD) de la Unión Europea. En muchos casos, los efectos del RGPD serán los mismos que para cualquier otro responsable o encargado. En algunas áreas, sin embargo, existen especificidades.

El RGPD fue publicado en mayo de 2016 y entró en vigor en ese mismo mes. Sin embargo, será aplicable a partir del 25 de mayo de 2018. Las modificaciones que deberán realizarse para alinear la actividad de las AALL con las previsiones del RGPD habrán de estar listas para aplicarse, a más tardar, en esa fecha de 2018.

El impacto del RGPD[1] sobre las AAPP puede sintetizarse en los siguientes puntos:

1. Necesidad de identificar con precisión las finalidades y la base jurídica de los tratamientos que llevan a cabo. La vigente LOPD parte de considerar que los tratamientos solo pueden llevarse a cabo con el consentimiento de los afectados, con una serie de excepciones entre las que se encuentra el que los datos sean recogidos por las AAPP para el ejercicio de sus funciones. Asimismo, la LOPD prevé que las cesiones de datos requerirán el consentimiento de los afectados salvo que, entre otras excepciones, esa cesión esté autorizada por una ley.

   El RGPD diseña un sistema de legitimación basado en seis bases jurídicas que no mantienen entre sí ninguna relación de prioridad o prelación. Entre esas bases jurídicas no se encuentran, en sentido estricto, los "fines propios de las AAPP en el ejercicio de sus competencias" ni la "autorización legal".

   Ello no supone en absoluto que los tratamientos amparados en esas bases de la legislación nacional no puedan seguir llevándose a cabo. Significa tan sólo que deberán encontrarse las bases jurídicas apropiadas para esos tratamientos dentro de las que el RGPD ofrece. En particular, y para el ámbito de las AALL, son relevantes las siguientes:

   - el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento

[1] Este Documento se refiere únicamente a efectos directamente derivados del RGPD como tal, aun cuando en ocasiones se hace referencia a las normas nacionales que deberán desarrollar algunas de sus previsiones. No se mencionan específicamente otras normas nacionales que podrán adoptarse en ejercicio de habilitaciones que contiene el propio RGPD y que podrían establecer determinadas condiciones adicionales para algunos tratamientos.

- el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento
- el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por un tercero al que el responsable comunica los datos [2]

La obligación de identificar y explicitar finalidades y bases legales de los tratamientos no deriva solo de la necesidad de cumplir con el principio de legalidad establecido en el RGPD, sino que viene impuesta por el hecho de que las finalidades o la base jurídica de los tratamientos son informaciones que deben proporcionarse a los interesados (arts. 13 y 14 RGPD) y recogerse en el registro de actividades de tratamiento.

Esta identificación tiene exigencias adicionales en los casos en que se traten datos de los considerados como objeto de especial protección, que incluyen, entre otros, los datos sobre salud, ideología, religión o pertenencia étnica. El tratamiento de estos datos está, con carácter general, prohibido, y sólo podrá llevarse a cabo si es aplicable alguna de las excepciones previstas en el art. 9.2 del RGPD. Entre ellas que pueden destacarse, a los efectos de este Documento, el que el tratamiento sea necesario para satisfacer un interés público esencial, el que sea necesario para fines de prevención, asistencia sanitaria o salud pública, o que sea necesario para la gestión de los servicios de asistencia social, en todos los casos en los términos en que establezca la legislación española o de la Unión Europea.

2. En el caso de la actividad de las AALL será muy habitual que la base jurídica de los tratamientos sea el cumplimiento de una tarea en interés público o el ejercicio de poderes públicos. Tanto el interés público como los poderes públicos que justifican el tratamiento deben estar establecidos en una norma. El Proyecto de futura Ley Orgánica de Protección de Datos (PLOPD) establece que esa norma deberá tener rango de ley formal.

3. En los casos en que la base jurídica de los tratamientos sea el consentimiento, éste deberá tener las características previstas por el RGPD, que exige que sea informado, libre, específico y otorgado por los interesados mediante una manifestación que muestre su voluntad de consentir o mediante una clara acción afirmativa.

   Los consentimientos conocidos como "tácitos", basados en la inacción de los interesados, dejarán de ser válidos a partir de la fecha de aplicación del RGPD, incluso para tratamientos iniciados con anterioridad. En estos casos, deberá encontrase una base jurídica adecuada dentro de las que ofrece el RGPD. Esta base puede ser el consentimiento inequívoco tal y como lo define el RGPD u otra que resulte apropiada a las circunstancias propias de cada tratamiento, como puede ser el cumplimiento de una

[2] En realidad, el RGPD menciona los intereses legítimos del responsable o de un tercero. Sin embargo, excluye expresamente que las autoridades públicas en el ejercicio de sus funciones puedan amparar sus tratamientos en esta base, por lo que para las AALL solo resulta aplicable respecto de terceros que no tengan esa condición de autoridades públicas.

misión de interés público o el ejercicio de poderes públicos. En todo caso, los afectados deben ser informados del cambio de base jurídica y deben poder ejercer los derechos asociados a la nueva base.

4. Necesidad de adecuar la información que se ofrece a los interesados cuando se recogen sus datos a las exigencias del RGPD (arts. 13 y 14). El RGPD obliga a ofrecer una información que es más amplia que la actualmente exigida por la Ley Orgánica de Protección de Datos. Obliga, además, a que esta información se proporcione de forma "concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo". Tanto esta obligación como la recogida en el siguiente punto requerirán la modificación de los documentos que actualmente recogen estas cláusulas informativas y la adaptación de los que se utilicen en el futuro en circunstancias como, por ejemplo, las convocatorias de subvenciones o de pruebas selectivas.

   La Agencia Española de Protección de Datos publicó en enero de 2017 una Guía para el cumplimiento del Deber de Informar en que se proponía ofrecer esta información en sucesivas capas. Este enfoque se recoge también en el PLOPD.

5. Necesidad de establecer mecanismos visibles, accesibles y sencillos, incluidos los medios electrónicos, para el ejercicio de derechos. Estos mecanismos, en particular cuando se trate del ejercicio por medios electrónicos, deben incorporar procedimientos para verificar la identidad de los interesados que los utilizan.

   El RGPD introduce varios nuevos derechos. De ellos, el que puede ejercerse más frecuentemente en el ámbito de las AALL es el de limitación del tratamiento. Este derecho supone que debe suspenderse el tratamiento de datos cuando los interesados soliciten la rectificación o supresión de sus datos personales hasta que el responsable decida sobre la solicitud.

   Los mecanismos para el ejercicio de derechos deben incluir los nuevos derechos.

6. Necesidad de establecer procedimientos que permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD. En algunos casos será preciso valorar la necesidad de que sean los encargados del tratamiento con los que se haya contratado la prestación de determinados servicios los que colaboren en la atención a las solicitudes de los interesados. En estos casos, esa colaboración debe incluirse en los contratos de encargo de tratamiento.

7. Necesidad de valorar si los encargados con los que se hayan contratado o se vayan a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD. El RGPD establece una obligación de diligencia debida en la elección de los encargados de tratamiento que deben aplicar todos los responsables, contratando únicamente encargados que estén en condiciones cumplir con el RGPD.

El RGPD establece que los encargados podrán demostrar esa disposición a cumplir con el RGPD mediante su adhesión a códigos de conducta o esquemas de certificación.

8. Necesidad de adecuar los contratos de encargo a las previsiones del RGPD. El RGPD establece que la relación entre responsables y encargados deberá formalizarse mediante un contrato o un acto jurídico que vincule al encargado. El RGPD exige expresamente que tanto los contratos como los actos jurídicos deberán tener un contenido mínimo que excede del actualmente previsto por la normativa española de protección de datos.

   Los contratos o actos jurídicos posteriores al 25 de mayo de 2018 deberán incluir ese contenido mínimo. El PLOPD establece un régimen transitorio para los contratos suscritos con anterioridad a esa fecha.

9. Necesidad de establecer un Registro de Actividades de Tratamiento. Este registro sustituye, en parte, a la obligación de notificar los ficheros y tratamientos a las autoridades de protección de datos.

   La importancia del registro en el momento en que comience a ser de aplicación el RGPD radica en que obliga a inventariar todos los tratamientos de datos que esté llevando a cabo cada entidad local.

   El RGPD establece un contenido mínimo de ese registro, tanto para responsables como para encargados de tratamiento, por lo que esa tarea de inventario debe incluir la identificación de todos los elementos que deben incorporarse al registro en relación con cada tratamiento.

   El registro podrá organizarse sobre la base de las informaciones ya proporcionadas en las notificaciones de los ficheros existentes. Para ayudar a su elaboración, la AEPD pone a disposición de los responsables la información sobre los ficheros notificados al Registro General de Protección de Datos.

   El registro deberá mantenerse actualizado y a disposición de las autoridades de protección de datos.

10. Necesidad de hacer un análisis de riesgo para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que se desarrollen. El RGPD hace depender la aplicación de todas las medidas de cumplimiento que prevé para responsables y encargados del nivel y tipo de riesgo que cada tratamiento implique para los derechos y libertades de los afectados. Por ello, todo tratamiento, tanto los ya existentes como los que se pretenda iniciar, deben ser objeto de un análisis de riesgos.

    En el contexto de las AAPP se dispone de metodologías de análisis de riesgos focalizadas principalmente en la seguridad de la información. Esas metodologías deben ampliarse para incluir riesgos asociados al incumplimiento de las disposiciones del RGPD. La AEPD está colaborando con el Centro Criptológico Nacional en esa

adaptación de las metodologías y herramientas de análisis y la versión definitiva estará a disposición de todas las AAPP.

11. Necesidad de revisar las medidas de seguridad que se aplican a los tratamientos a la luz de los resultados del análisis de riesgo de los mismos. La normativa española de protección de datos contiene previsiones específicas sobre medidas de seguridad atendiendo básicamente al tipo de datos que se tratan. El RGPD, sin embargo, deja sin efecto esas previsiones, en la medida en que exige que las medidas de seguridad se adecúen a las características de los tratamientos, sus riesgos, el contexto en que se desarrollan, el estado de la técnica y los costes.

    En el caso de las AAPP, incluidas las AALL, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad. El Esquema está siendo revisado para adaptarlo a las exigencias del RGPD, dado que en su versión actual las medidas de seguridad para datos personales que recogía se remitían a las previsiones de la normativa de protección de datos que, como se ha indicado, no son válidas a la luz del RGPD.

12. Necesidad de establecer mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos y reaccionar ante ellas, en particular para evaluar el riesgo que puedan suponer para los derechos y libertades de los afectados y para notificar esas violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados. El RGPD establece, asimismo, la obligación de mantener un registro de todos los incidentes de seguridad, sean o no objeto de notificación.

13. Necesidad de valorar si los tratamientos que se realizan requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados y de disponer de una metodología para la llevarla a cabo. El RGPD establece que, con anterioridad a su puesta en marcha, los tratamientos que sea probable que supongan un alto riesgo para los derechos y libertades de los afectados deberán ser objeto de una Evaluación de Impacto sobre la Protección de Datos. El RGPD determina algunos de los casos en que se presumirá que existe ese alto riesgo y prevé que las autoridades nacionales de protección de datos publiquen listas de otros tratamientos de alto riesgo. También contempla un contenido mínimo de las Evaluaciones de Impacto.

    En el caso de tratamientos basados en la consecución de fines de interés público o vinculados al ejercicio de poderes públicos, el RGPD prevé que pueda no llevarse a cabo la Evaluación de Impacto, pese a tratarse de tratamientos de alto riesgo, cuando la norma de base regule la operación o conjunto de operaciones de tratamiento y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de esa norma de base.

14. Necesidad de designar un Delegado de Protección de Datos (DPD). El RGPD prevé que todas las "autoridades u organismos públicos" nombrarán un DPD. También establece cuáles habrán de ser los criterios para su designación (cualidades profesionales y conocimientos en derecho y práctica de la protección de datos), su posición en la organización y sus funciones. Prevé, igualmente, que en el caso de las autoridades u organismos públicos puedan nombrarse un único DPD para varios de ellos, teniendo en cuenta su tamaño y estructura organizativa.

    En el ámbito de las AALL las dimensiones de las organizaciones harán inviable en muchos casos que una entidad local cuente con un DPD integrado en su plantilla, ya sea a tiempo completo o a tiempo parcial. Por ello, será preciso encontrar soluciones que permitan que los entes locales cumplan las obligaciones del RGPD en este punto de una forma que se adapte a sus especiales características. Entre las posibles opciones se encuentra la contratación de la actividad de DPD por parte de varias entidades como prestación de servicios o el establecimiento de servicios de DPD a disposición de los municipios en las Diputaciones Provinciales.

    En todo caso, debe asegurarse que los DPD designados reúnen los requisitos de cualificación y competencia establecidos por el RGPD y que su actividad en relación con las entidades en las que desempeñen sus funciones debe también seguir los criterios marcados por el RGPD.

    La designación del DPD debe comunicarse a las autoridades de protección de datos. Asimismo, deben establecerse mecanismos para que los interesados puedan contactar con el DPD.

15. Necesidad de adaptar los instrumentos de transferencia internacional de datos personales a las previsiones del RGPD. El RGPD mantiene el modelo de transferencias internacionales ya existente, pero amplía el catálogo de instrumentos para ofrecer garantías suficientes que no requerirán de autorización previa de las autoridades de protección de datos.

    Podría parecer que este tipo de transferencia será poco habitual en el ámbito de las AALL. Sin embargo, el uso cada vez más frecuente de tecnologías de la información y la comunicación o la generalización de la prestación de servicios "en nube" hacen que aumenten las posibilidades de que los datos se transfieran fuera de la Unión Europea.

    Dependiendo del tipo de prestación, los responsables en el ámbito de la administración local deberían tener en cuenta esas posibles implicaciones internacionales y la necesidad de que esas transferencias se lleven a cabo sobre la base de los adecuados instrumentos.