AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

EL IMPACTO DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS SOBRE LA ACTIVIDAD DE LAS ADMINISTRACIONES PUBLICAS

Las Administraciones Públicas (AAPP) 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 para el sector público.

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 normativa y la práctica de las AAPP 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. Esta obligación no deriva sólo 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.

   La identificación de finalidades y base jurídica 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 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 que establezca la legislación española o de la Unión Europea.

[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.

2. En el caso de la actividad de las AAPP 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 de rango legal.

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.

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.

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.

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.

8. Necesidad de adecuar los contratos de encargo que actualmente se tengan suscritos 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. En el caso de las AAPP será frecuente que el encargo de tratamiento se establezca mediante actos jurídicos, por ejemplo en la norma de creación de órganos encargados de la prestación de servicios informáticos. 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.

9. 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.

10. 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. El RGPD establece un contenido mínimo de ese registro, tanto para responsables como para encargados de tratamiento. El registro podrá organizarse sobre la base de las informaciones ya proporcionadas en las notificaciones de los ficheros existentes. El registro deberá mantenerse actualizado y a disposición de las autoridades de protección de datos.

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. Puede ocurrir que, tras un análisis de riesgo, y tomando en cuenta todos los demás factores, las medidas de seguridad sean las mismas que la normativa española prevé para un tipo determinado de datos. Pero en todo caso la aplicación de esas medidas no puede derivarse automáticamente de que se traten unos datos u otros, sino que ha de ser la consecuencia de un análisis de riesgos específico para cada tratamiento. En el caso de las AAPP, la aplicación de las medidas

de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad.

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 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 consecuencia, como medida previa deben identificarse las unidades en que se integrar el DPD dentro de cada órgano u organismo, su posición en la estructura administrativa y los mecanismos para asegurar que los DPD designados reúnen los requisitos de cualificación y competencia establecidos 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. Entre estos instrumentos se incluyen los jurídicamente vinculantes y exigibles entre autoridades y organismos públicos. También prevé expresamente que requerirán autorización las transferencias basadas en acuerdos no jurídicamente vinculantes.