



Por medio de la presente, le informo que a partir del próximo 25 de mayo de 2018 será de aplicación directa en todas las entidades locales el Reglamento General de Protección de Datos (en adelante RGPD), aprobado mediante Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que introduce una serie de novedades que afectan a los Ayuntamientos. El objetivo es intentar dar una breve información que sirva de aproximación a los nuevos cambios normativos.

Los Reglamentos europeos, a diferencia de las directivas, son directamente aplicables sin necesidad de legislación nacional adicional, debido a que por su propia naturaleza una vez que entran en vigor pasan a formar parte del derecho interno, por tanto el RGPD es una norma directamente aplicable, la cual no requiere de normas internas de trasposición, si bien puede ser desarrollada por la Ley que sustituya a la actual Ley Orgánica de Protección de Datos (LOPD), cuyo estado de tramitación se encuentra actualmente en Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal.

Sin perjuicio de una lectura más detallada del Reglamento, señalar que en el ámbito de las Corporaciones Locales, antes de la entrada en vigor del reglamento, se deberán tener en cuenta, como mínimo las siguientes consideraciones básicas:

1. Necesidad de establecer un Registro de Actividades de Tratamiento.

El RGPD establece en su art. 30 la obligación de llevar y mantener actualizado y a disposición de las autoridades de protección de datos un Registro de Actividades de Tratamiento, cuyo contenido refleja el mencionado precepto. Este registro sustituye a la obligación de notificar los ficheros y tratamientos a las autoridades de protección de datos, que desaparece tras la reforma. El registro podrá organizarse sobre la base de las informaciones ya proporcionadas en las notificaciones de los ficheros existentes.

2. Necesidad de identificar las finalidades y bases jurídicas de los tratamientos.

En todas las entidades locales se deben identificar con precisión las finalidades y la base jurídica de los tratamientos de datos de carácter general que se llevan a cabo. Esta obligación se deriva de la necesidad de cumplir con el principio de legalidad establecido en el RGPD y 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.

En la actuación 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, pero en uno y otro caso es preciso que el tratamiento tenga fundamento en una norma de rango legal.

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.

3. Obligación de revisar y adecuar la información sobre protección de datos.

Se debe revisar y adecuar a las exigencias del RGPD la información que se ofrece a los interesados cuando se recogen sus datos a las exigencias del RGPD y los medios para el ejercicio de sus derechos en la materia. El RGPD obliga a ofrecer una información más amplia que la actualmente exigida por la Ley Orgánica de Protección de Datos.

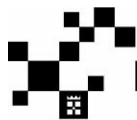
Además, esta información se debe proporcionar de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, lo que exige la revisión y modificación de los documentos que actualmente recogen cláusulas informativas.

4. Obligación de designar un Delegado de Protección de Datos (DPD).

El RGPD dispone en su art. 37 que todas las autoridades u organismos públicos deben nombrar un DPD y comunicarlo a las autoridades de protección de datos.

En sus artículos siguientes fija 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.

Es relevante especialmente en el ámbito local el hecho de que el RGPD prevea la posibilidad de que los organismos públicos puedan nombrar un único DPD para varios de ellos, teniendo en cuenta su tamaño y estructura organizativa. La viabilidad de esta nueva figura en



los pequeños y medianos ayuntamientos debe ser considerada en ese contexto, y contar con el impulso de las Diputaciones Provinciales, como una proyección más de su responsabilidad de asistencia técnica a los ayuntamientos de menor capacidad económica y de gestión que le atribuye el art. 36 LRBRL legalmente atribuida a las Diputaciones provinciales, como ya está impulsando la AEPD.

El Delegado de Protección de Datos podrá formar parte de la plantilla interna de la Administración Local a tiempo completo o parcial o incluso desempeñar sus funciones en el marco de un contrato de servicios.

Por tanto, esta segunda posibilidad permite que se contraten externamente las funciones de Delegado de Protección de Datos, considerando esta opción la más ventajosa para los pequeños municipios puesto que podrán beneficiarse de los servicios que, en su caso, ofrezcan la diputación provincial o la comunidad autónoma, así como contratar servicios de entidades privadas especializadas.

Este Delegado será designado atendiendo a sus cualidades profesionales, a sus conocimientos especializados del derecho y la práctica en materia de protección de datos.

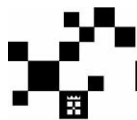
El método de evaluación se basará tanto en la valoración del conocimiento y experiencia, como en el desarrollo profesional continuo. La provisión de los puestos de trabajo requerirá la selección de empleados públicos que reúnan tales requisitos.

La Agencia Española de Protección de Datos ha optado por promover un sistema de certificación de Delegado de Protección de Datos en el cual el candidato deberá justificar la experiencia profesional en materia de protección de datos, así como superar una prueba de evaluación teórica mediante la realización de un examen.

En estos términos recomendamos acudir al [Esquema de Certificación de Delegados de Protección de Datos publicado por la Agencia de Protección de datos.](#)

La certificación no es la única vía para adquirir la condición de Delegado, si bien la Agencia Española de Protección de Datos ha considerado necesario ofrecer tal posibilidad para que sirva de base para su nombramiento y de esta forma garantizar la cualificación y capacidad de los candidatos a Delegado de Protección de Datos. Sin embargo, los responsables pueden determinar otros medios para determinar la competencia de los Delegados de Protección de Datos.

Una vez designado el Delegado de Protección de Datos, los responsables o encargados deberán publicar sus datos de contactos y



comunicarlos a la autoridad de control.

En lo relativo a las funciones del Delegado destacamos:

- Informar y asesorar al responsables en lo relativo al cumplimiento de las obligaciones dispuestas en el RGPD.
- Actuar como punto de contacto entre la autoridad de control, los responsables o encargados del tratamiento y los interesados en todo lo que tenga relación con el tratamiento de sus datos personales.
- Supervisar el cumplimiento de las obligaciones dispuestas en el RGPD.

Asimismo, el Delegado está obligado a mantener el secreto o la confidencialidad en el desarrollo de sus funciones, así como a no recibir ninguna instrucción durante el desempeño de las mismas.

El Delegado podrá desempeñar otras funciones, siempre que las mismas no den lugar a conflicto de intereses.

5. Obligación de hacer un análisis de riesgo para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que se desarrollen y de revisar las medidas de seguridad.

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 debe ser objeto de un análisis de riesgos y, tras ello, el RGPD exige que se establezcan las medidas de seguridad adecuadas 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, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad.

Asimismo, se deben 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.

6.- Contratos de encargo.

El contrato de encargo es el documento que determina los



derechos y obligaciones de las partes entre responsable del tratamiento de datos y el encargado.

En caso que se realizare tal contrato de encargo por la Administración Local responsable del tratamiento de datos, el mismo deberá respetar el contenido mínimo citado en el artículo 28 del RGPD y deberá constar pos escrito, inclusive en formato electrónico. Destacamos aspectos como:

- Tratamiento de los datos personales únicamente siguiendo instrucciones documentadas del responsable.

- Asistencia y ayuda al responsable por parte del encargado.

- Garantía de la confidencialidad de dicho tratamiento.

- Subcontratación: en caso que un encargado recurra a otro encargado para llevar a cabo actividades de tratamiento se realizará el mediante nuevo contrato u otro acto jurídico con las mismas obligaciones de protección de datos estipuladas en el contrato entre responsable y encargado. Si ese otro encargado incumple tales obligaciones, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento.

Se deberán revisar los contratos ya existentes para adaptarlos al RGPD, así como incluir las nuevas cláusulas contractuales en los contratos que se vayan elaborando ofreciendo las garantías de cumplimiento del RGPD.

No obstante, la responsabilidad última sobre el tratamiento sigue estando atribuida el responsable.

Lo que informo para su conocimiento y efectos oportunos.

Teruel, 31 de enero de 2018.

La Diputada Delegada SATM

(Presidencia, Diputada Delegada SATM)