CONSIDERACIONES DE URGENCIA ANTE LA INMINENTE ENTRADA EN VIGOR DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS.

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 (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.

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.

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.

LUIS JESUS DE JUAN CASERO

Vicesecretario General de la Diputación de Ciudad Real