LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

NUEVAS OBLIGACIONES PARA EL SECTOR PÚBLICO

1. Publicación del Registro de actividades de tratamiento del órgano u organismo del Sector Público

Los órganos y organismos del Sector Público quedan obligados a publicar en su página **web** el inventario de las actividades de tratamiento de datos personales que realizan, identificando **quién trata los datos, con qué finalidad y qué base jurídica** legitima ese tratamiento.

2. Obligación de información a los ciudadanos sobre el ejercicio de sus derechos

Los órganos y organismos del Sector Público quedan obligados a incluir en su página **web** información clara y precisa destinada a los administrados sobre el ejercicio de los **derechos de acceso, rectificación, supresión, derecho a la limitación del tratamiento, así como a la portabilidad y oposición.**

3. Potestad de verificación de los datos personales de los ciudadanos

Los órganos y organismos del Sector Público pueden **verificar**, **sin** necesidad de solicitar **consentimiento del interesado**, la exactitud de los **datos personales** manifestados por los ciudadanos que obren en poder de los órganos y organismos del Sector Público.

4. Nueva regulación de la aportación de documentación por parte de los ciudadanos: modificación del artículo 28 de la Ley 39/2015

Ya la ley 30/1992 reconocía a los administrados el derecho a no aportar a los procedimientos administrativos los documentos que obrasen en poder de la Administración, o que hubiesen sido elaborados por ésta. La base jurídica del tratamiento de los datos personales por la Administración era el consentimiento del administrado, que se entendía tácitamente concedido si el interesado no se oponía expresamente.

Tanto el Reglamento General de Protección de Datos como la nueva Ley Orgánica **eliminan la necesidad de recabar el consentimiento, ni siquiera tácito, del ciudadano**, al establecer como base jurídica legitimadora principal del tratamiento de datos personales por órganos y organismos del Sector Público **el cumplimiento de una misión en interés público o, particularmente, el ejercicio de poderes públicos.**

Asimismo, la nueva redacción otorgada por la Ley Orgánica al artículo 28 de la Ley 39/2015 **reconoce al interesado la posibilidad de oponerse** a que órganos y organismos del Sector Público consulten o recaben los citados documentos, pero en ese caso el administrado deberá aportarlos necesariamente para que la Administración pueda conocer que concurren en él los requisitos establecidos por la norma. En caso contrario no podrán estimar su solicitud, precisamente porque no habría demostrado los requisitos requeridos.

En todo caso, dicho derecho de oposición no juega en los casos de potestades de verificación o inspección.

5. Notificación de actos administrativos: identificación de los ciudadanos

La nueva Ley **impide el uso conjunto apellidos, nombre y número completo del documento de identificación oficial** de las personas en aquellos actos administrativos que vayan a ser objeto de publicación o notificación por medio de anuncios.

A partir de la entrada en vigor de la Ley Orgánica:

- **Cuando un acto administrativo se deba publicar** se identificará a la persona mediante su **nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias** de su documento identificativo oficial.
- Cuando se trate de **notificaciones** por medio de anuncios se identificará a la persona exclusivamente con el **número de su documento identificativo**

En ambos casos, **cuando la persona carezca de documento identificativo se la identificará sólo mediante su nombre y apellidos.**

6. Comunicación de datos personales de los administrados a sujetos privados

Los órganos y organismos del Sector Público pueden **comunicar** los datos personales de los administrados a **sujetos de derecho privado** que lo soliciten:

a) o bien cuando cuenten con el **consentimiento** de los administrados.

b) o bien, cuando aprecien que **concurre** en el sujeto privado solicitante un **interés legítimo que prevalezca** sobre los derechos e intereses de los administrados concernidos.

7. Designación de un Delegado de Protección de Datos (DPD) y comunicación de la designación a la AEPD

Los órganos y organismos del Sector Público tienen obligación de **designar un Delegado** de Protección de Datos que cuente con la debida cualificación, de **garantizarle los medios** necesarios para el ejercicio de sus funciones y de **notificar** la designación a la **AEPD** para su inclusión en el **Registro público de Delegados** de Protección de Datos.

El Delegado de Protección de Datos no tiene responsabilidad a título personal, por este mero hecho, por las posibles infracciones en materia de protección de datos cometidas por su organización.

8. Intervención del Delegado de Protección de Datos en la resolución de reclamaciones en el Sector Público

El Delegado de Protección de Datos del órgano u organismo del Sector Público debe recibir las reclamaciones que les dirijan los administrados, cuando opten por esta vía antes de plantear una reclamación ante la AEPD, y comunicará la decisión adoptada al administrado en el plazo máximo de dos meses.

Asimismo, el Delegado de Protección de Datos deberá recibir las **reclamaciones que la AEPD decida trasladarle con carácter previo al inicio de un expediente sancionador**. El Delegado debe comunicar la decisión adoptada al administrado y a la AEPD en el plazo máximo de un mes.

De esta forma, con carácter general, si el Delegado de Protección de Datos consigue que el responsable resuelva por cualquiera de estas dos vías la

reclamación, y sin perjuicio de que el interesado posteriormente se dirija a la AEPD, no se iniciaría expediente de declaración de infracción a esa Administración Pública.

9. Mayor transparencia de las sanciones impuestas al Sector Público

Las infracciones cometidas por los órganos y organismos del Sector Público serán sancionadas con un apercibimiento con medidas correctoras y no tendrán sanción económica.

La resolución sancionadora de la AEPD identificará el cargo responsable de la infracción, se notificará al infractor, a su superior jerárquico, al Defensor del Pueblo y se publicará en la página web de la AEPD y en el diario oficial correspondiente.

La resolución sancionadora podrá proponer al órgano u organismo la iniciación de actuaciones disciplinarias, cuya resolución deberá ser comunicada por el órgano u organismo del Sector Público a la AEPD.

Las infracciones sean imputables a autoridades y directivos del Sector Público y se acredite la existencia de informes técnicos o recomendaciones que no hubieran sido atendidos por estos, la resolución sancionadora incluirá una amonestación con la identificación del cargo responsable y se publicará en el diario oficial correspondiente.

10. Tratamiento de datos personales en la notificación de incidentes de seguridad

Las autoridades públicas, los equipos de respuesta a emergencias informáticas (CERT), los equipos de respuesta a incidentes de seguridad informática (CSIRT), los proveedores de redes y servicios de comunicaciones electrónicas y los proveedores de tecnologías y servicios de seguridad pueden tratar los datos personales contenidos en las notificaciones de incidentes de seguridad **exclusivamente durante el tiempo y alcance necesarios** para su análisis, detección, protección y respuesta, adoptando siempre las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo.

11. Registros de personal del sector público: legitimación del tratamiento

La nueva Ley Orgánica establece que la base legitimadora del tratamiento de datos personales que realizan los registros de personal del sector público es el ejercicio de potestades públicas.

Estos registros pueden tratar los datos personales que sean estrictamente necesarios para el cumplimiento de sus fines relativos a infracciones y condenas penales e infracciones y sanciones administrativas, de los que deberán ser informados de manera expresa, clara e inequívoca.

12. Derechos de los empleados públicos: mayor intimidad

La Ley Orgánica garantiza el derecho a la intimidad de los empleados públicos en el lugar de trabajo frente al uso de dispositivos de videovigilancia y de grabación de sonidos, así como frente al uso de los dispositivos digitales y sistemas de geolocalización.

13. Adaptación a la Ley Orgánica de los contratos de encargo de tratamiento de datos personales

Los contratos de encargo de tratamiento de datos personales entre los órganos y organismos del Sector Público (como responsables) y otros órganos u organismos del sector público o terceros (como encargados de tratamiento) suscritos antes del 25 de mayo de 2018 mantendrán su vigencia como máximo hasta el 25 de mayo de 2022.

14. Tratamiento de datos personales por concesionarios de servicios públicos

Los órganos y organismos del Sector Público mantendrán el control sobre los datos personales de los usuarios de los servicios públicos aunque haya finalizado la vigencia del contrato de concesión de servicios.

En el Sector Público, un concesionario de servicios, encargado del tratamiento de datos personales, no se convierte nunca en responsable aunque establezca relaciones con las personas a cuyos datos ha accedido en virtud de la prestación del servicio.

15. Educación para la digitalización

El Gobierno debe remitir en el plazo de un año desde la entrada en vigor de la Ley Orgánica un proyecto de ley dirigido a garantizar un uso de los medios digitales que sea seguro y adecuado.

Las Comunidades Autónomas dispondrán del mismo plazo para incluir en los currículos los contenidos precisos para garantizar la plena inserción del alumnado en la sociedad digital y asegurar una formación adecuada de todo el personal docente.

16. Tratamiento de datos personales en investigación sanitaria

La nueva Ley Orgánica flexibiliza el tratamiento de datos para la investigación en salud:

- amplía las finalidades para las que se puede otorgar el consentimiento al tratamiento,
- recoge la posibilidad de reutilizar la información sobre la que se ya se haya prestado consentimiento con anterioridad,
- recoge el uso de datos pseudonimizados como una opción para facilitar la investigación sanitaria incluyendo garantías para evitar la reidentificación de los afectados,
- regula las garantías de este tratamiento, incluyendo la intervención de los Comités de Ética de la Investigación o, en su defecto, del Delegado de Protección de Datos o de un experto en protección de datos personales.

Diciembre 2018