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

NOVEDADES PARA EL SECTOR PRIVADO

1. Obligación de información a los ciudadanos sobre el tratamiento de sus datos y sobre el ejercicio de sus derechos

Las organizaciones quedan obligadas a informar a los ciudadanos de forma clara y sencilla sobre los aspectos más importantes del tratamiento de sus datos, identificando **quién trata los datos, con qué base jurídica para qué finalidad, y sobre la forma de ejercer los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad, oposición y decisiones automatizadas, incluida la elaboración de perfiles.**

Las organizaciones no podrán denegar el ejercicio de estos derechos en el caso de que el ciudadano quiera ejercitarlos de un modo diferente al que se le ofrezca.

Las organizaciones que traten datos de carácter básico pueden utilizar la herramienta gratuita FACILITA para su adaptación al Reglamento General de Protección de Datos.

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

La Ley obliga a las organizaciones cuyas actividades principales consistan en tratamientos que requieran una observación habitual y sistemática de los ciudadanos a gran escala, o en el tratamiento a gran escala de categorías especiales de datos personales, o datos relativos a condenas e infracciones penales a **designar un** Delegado de Protección de Datos que cuente con la debida cualificación, a **garantizarle los medios** necesarios para el ejercicio de sus funciones y a **notificar** la designación a la **AEPD** para su inclusión en el **Registro público de Delegados de Protección de Datos**.

En el resto de los supuestos, la designación de un Delegado de Protección de Datos será voluntaria.

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.

3. Intervención del Delegado de Protección de Datos en la resolución de reclamaciones

El Delegado de Protección de Datos debe recibir las reclamaciones **que le dirijan los ciudadanos**, cuando opten por esta vía antes de plantear una reclamación ante la AEPD, y comunicará la decisión adoptada al particular en el plazo máximo de dos meses.

Asimismo, el Delegado 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 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.

4. Las bases jurídicas que legitiman el tratamiento de datos personales de los ciudadanos por parte de las organizaciones

El Reglamento General de Protección de Datos y la Ley Orgánica recogen varias bases jurídicas legitimadoras del tratamiento de datos personales por parte de las organizaciones privadas: relación contractual previa que contemple el tratamiento, consentimiento del ciudadano o interés legítimo que prevalezca sobre los derechos de las personas, entre otras.

Por tanto, en la actualidad, **no resulta necesario que el particular consienta el tratamiento de sus datos personales si existe otra base jurídica que legitime el tratamiento.**

En los casos en los que el consentimiento del ciudadano sea preciso por no existir otra base legitimadora, la Ley establece que debe ser una manifestación de voluntad libre, específica, informada e inequívoca por la que una persona acepta el tratamiento de sus datos personales, ya sea mediante una declaración o una clara acción afirmativa. Se excluye el consentimiento tácito o por omisión.

Además, cuando se pretenda que el consentimiento del ciudadano legitime un tratamiento para una variedad de finalidades, será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

No podrá denegarse un contrato o la prestación de un servicio por el hecho de que la persona no consienta el tratamiento de sus datos personales para finalidades que no guarden relación con ese contrato o con la prestación de ese servicio.

5. Tratamiento de datos de menores de edad

En el caso de datos personales de menores, cuando el tratamiento de datos esté legitimado por el consentimiento, la organización debe recabar el consentimiento del menor cuando este tenga al menos 14 años; y el de los padres o sus representantes legales en el caso de que sea menor de 14 años.

6. Limitación de la actividad publicitaria: las "listas Robinson"

Las entidades que vayan a realizar una campaña publicitaria deben consultar con carácter previo las "listas Robinson" para evitar el envío de publicidad a todos los ciudadanos que se hayan registrado en ellas.

No será preciso realizar esta consulta en el caso de los ciudadanos que hayan dado su consentimiento para recibir publicidad de una entidad, tanto si lo dieron antes como si lo hicieron después de registrarse en dicha lista.

7. Derechos de los empleados: mayor intimidad

La Ley Orgánica garantiza el derecho a la intimidad de los empleados 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, de los que deberán ser informados de forma expresa, clara e inequívoca.

8. Datos de contacto profesionales: legitimación de su tratamiento

La Ley permite utilizar los datos personales de contacto de las personas que prestan servicios en una entidad, así como de los profesionales (abogados, médicos, etc.) y de los empresarios individuales, siempre que se traten con la finalidad de mantener contacto con la entidad en la que prestan sus servicios o de establecer contacto con fines profesionales o empresariales.

9. Sistemas de denuncias internas: exención de responsabilidad penal de las organizaciones

La Ley recoge los sistemas de denuncia interna, incluso anónima, como mecanismo para que los integrantes de una organización puedan poner en su conocimiento, la comisión de infracciones en su seno que pudieran resultar contrarias a la normativa general o sectorial que le fuera aplicable.

10. Inclusión en sistemas de información de solvencia crediticia ("ficheros de morosos")

Los ciudadanos podrán ser incluidos en los sistemas de información de solvencia crediticia cuando mantengan una deuda de más de 50 euros con algún prestador de servicios (la ley anterior no establecía ninguna cuantía mínima).

Los ciudadanos no podrán mantenerse registrados en estos sistemas más de 5 años, contados desde la fecha de vencimiento de la obligación de pago (la ley anterior establecía un plazo de 6 años).

La Ley establece que se podrán consultar estos sistemas de información:

- cuando quien consulte tenga una relación contractual con la persona y esta relación implique el abono de una cuantía concreta,
- cuando la persona hubiera solicitado financiación, pago aplazado o facturación periódica.

Si como consecuencia de la consulta realizada se denegase la solicitud de celebración del contrato o este no llegara a celebrarse, quien haya consultado deberá informar al afectado del resultado de la consulta.

11. Novedades sobre videovigilancia

- **Captación de la vía pública:** Sólo podrán captarse imágenes de la vía pública cuando resulte imprescindible para preservar la seguridad de las personas y los bienes, así como de sus instalaciones.

  No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicas o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

- **Supresión de los datos:** Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando tuvieran que conservarse para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

- **Deber de información:** El deber de información en el caso de videovigilancia se cumplirá colocando un dispositivo informativo en un lugar suficientemente visible que identifique, al menos, la existencia del tratamiento, la identidad del

responsable y la posibilidad de ejercitar los derechos. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información. En este enlace puede consultarse el modelo de cartel de videovigilancia realizado por la Agencia Española de Protección de Datos.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los ciudadanos la información especificada en el punto 1 de este documento.

12. Operaciones mercantiles

La Ley establece que se presumirán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios.

En el caso de que la operación no llegara a concluirse, la entidad cesionaria deberá proceder con carácter inmediato a la supresión de los datos, sin que sea de aplicación la obligación de bloqueo.

13. La obligación de bloqueo de los datos personales tras el ejercicio de los derechos de rectificación o supresión

El responsable del tratamiento, cuando proceda a la rectificación o supresión de los datos, está obligado a bloquearlos; es decir, a identificarlos y reservarlos mediante técnicas que impidan su tratamiento, visualización incluida.

Cuando el bloqueo de esos datos no fuese técnicamente posible o resultara antieconómico, se procederá a un copiado seguro de la información para que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la información, la fecha del bloqueo y la no manipulación de los datos.

El bloqueo de los datos personales sólo permitirá su puesta a disposición de jueces y tribunales, Ministerio Fiscal o Administraciones públicas competentes (como la AEPD), para la exigencia de eventuales responsabilidades derivadas del tratamiento y sólo por el plazo de prescripción de las mismas. Transcurrido ese plazo, deberá procederse a la destrucción de los datos.

14. 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.

15. 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 las organizaciones (como responsables) y 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.

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.

17. Modificación de la Ley 3/1991, de 10 de enero, de Competencia Desleal: prácticas agresivas

Se recoge como práctica agresiva en la Ley de Competencia Desleal la suplantación de identidad de la Agencia Española de Protección de Datos o de sus funciones y el asesoramiento conocido como "adaptación al Reglamento con coste 0", a fin de limitar los asesoramientos ofrecidos por empresas con servicios de ínfima calidad.

Diciembre 2018