La gestión del dato y la LOPD

EXPONENT CONSULTORES

EL NUEVO REGLAMENTO DE LA UE

“

Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial.
La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

.”

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016

Obtención del consentimiento para el tratamiento de datos

Normativa actual (LOPD): La actual LOPD exige el consentimiento inequívoco de los interesados para el tratamiento de sus datos. No obstante, si los datos recabados no son especialmente sensibles, se admite que dicho consentimiento pueda ser tácito, tal y como se establece en el Informe Jurídico 0645/2009 emitido por la Agencia Española de Protección de Datos. Por otra parte, en relación con el tratamiento de datos de menores, la LOPD establece, salvo excepciones legales, la posibilidad de recabar datos personales de mayores de 14 años sin necesidad de recabar el consentimiento de sus padres.

Normativa futura (RGPD): El RGPD mantendrá los mismos principios del consentimiento que establece la LOPD, exigiendo un consentimiento libre, informado, específico e inequívoco. Sin embargo, como novedad respecto de la LOPD, indica que para poder considerar que el consentimiento es inequívoco, deberá existir una declaración del interesado o una acción positiva que manifieste su conformidad. El silencio, las casillas ya marcadas o la inacción no constituirán prueba de consentimiento (Considerando 32 del RGPD).

Deber de información

Normativa actual (LOPD): Nuestra legislación actual establece la obligación de informar en todo proceso de recogida de datos personales sobre la existencia de un fichero o tratamiento de datos de carácter personal, la identidad del responsable del tratamiento, la finalidad de la recogida de los datos y de los destinatarios de la información, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. Asimismo, cuando los datos personales se hayan obtenido de terceros, el responsable del tratamiento dispondrá de un **plazo de tres meses** para informar al interesado, debiendo indicar la procedencia de los datos.

Normativa aplicable en 2018 (RGPD): El Reglamento establece la **obligación de informar sobre nuevos aspectos**. Por ejemplo, habrá que explicar la base legal para el tratamiento de los datos, el período de conservación de los mismos y que los interesados podrán dirigir sus reclamaciones a las Autoridades de protección de datos, si consideran que hay un problema con la forma en que están manejando sus datos. En lo que respecta al interesado cuyos **datos se han obtenido de otra fuente**, la información anteriormente indicada deberá facilitarse en el **plazo de máximo de un mes** (en lugar de los tres meses indicados en la LOPD).

Ejercicio de derechos

Normativa actual (LOPD): los derechos reconocidos en la actual LOPD son los siguientes:

Derecho de acceso,
Derecho de rectificación,
Derecho de oposición,
Derecho de cancelación.

Normativa futura (RGPD): En el RGPD se incluyen, además de los anteriores, los siguientes derechos:

Derecho a la transparencia de la información,
Derecho de supresión (derecho al olvido),
Derecho de limitación,
Derecho de portabilidad.

Otra novedad, respecto de la LOPD, es que se establece la obligación para el responsable del tratamiento de proporcionar medios para que las solicitudes de ejercicio de derechos se presenten por medios electrónicos, en particular cuando los datos personales se hayan recabado a través de estos medios (Considerando 59).

Comunicación de fallos a la autoridad de protección de datos

Normativa actual (LOPD): No se regula en la LOPD.

Normativa aplicable en 2018 (RGPD): Se trata de una nueva obligación del RGPD que impone al responsable del tratamiento la obligación de notificar los fallos de seguridad que se produzcan en su organización, a la Agencia Española de Protección de Datos (AEPD) en un plazo de 72 horas. El responsable del tratamiento debe contar con un sistema efectivo para realizar el reporte a la AEPD o para comunicar el fallo a los afectados si existe algún riesgo para sus derechos.

Registro de tratamiento de datos

Normativa actual (LOPD): No se regula en la LOPD.

Normativa aplicable en 2018 (RGPD): Según lo previsto en el artículo 30 del RGPD, las organizaciones que habitualmente realicen tratamiento de datos de riesgo para la privacidad de los interesados, o traten datos sensibles, deberán contar con un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener información relativa, entre otros aspectos, a los tratamientos de datos que se realicen, los datos personales que se traten, los destinatarios de los datos, los plazos previstos para la supresión, la finalidad de dicho tratamiento y las medidas técnicas y de seguridad adoptadas por la empresa para realizar dicho tratamiento.

Privacidad desde el diseño y por defecto, códigos de conducta y esquemas de certificación

Normativa actual (LOPD): No se regula en la LOPD.

Normativa aplicable en 2018 (RGPD): Se avanza un paso más para reforzar el concepto de accountability empresarial, es decir, la responsabilidad proactiva en el cumplimiento normativo. Para ello, el RGPD establece la privacidad desde el diseño y por defecto, con el fin de que se garantice el cumplimiento con carácter previo al tratamiento de datos y durante dicho tratamiento. Asimismo, el RGPD propone como mecanismos efectivos de verificación del cumplimiento, la adhesión a códigos de conducta o a mecanismos de certificación (artículo 42.3 del RGPD).

EL DPO Y EL ANÁLISIS DE RIESGOS

Evaluación de impacto del tratamiento de datos personales

Normativa actual (LOPD): No se regula en la LOPD.

Normativa aplicable en 2018 (RGPD): Se establece la obligación de realizar una evaluación de impacto (P*rivacy Impact Assesment*) para las organizaciones que realicen tratamientos de datos que puedan implicar un alto riesgo para los derechos y libertades de las personas físicas, en la que se evalúe el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo (Considerando 84 del RGPD).

Aplicación de medidas de seguridad

Normativa actual (RLOPD): Actualmente el RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RLOPD) establece la obligación de aplicar diferentes medidas de seguridad, en función del nivel básico, medio o alto de los datos tratados. Dichas medidas se concretan y describen en el Documento de Seguridad.

Normativa aplicable en 2018 (RGPD): El RGPD ya no distingue entre ficheros de nivel básico, medio o alto, sino que especifica que las medidas de seguridad se aplicarán teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas. La nueva legislación habla de "*medidas técnicas y organizativas apropiadas*" para garantizar un nivel de seguridad adecuado al riesgo, pero no concreta qué tipo de medidas deben aplicarse, a diferencia de lo que ocurre con el actual RLOPD que describe de manera detallada cada medida de seguridad que debe implementar el responsable del tratamiento.

Delegado de protección de datos DPO

Normativa actual (RLOPD): El RLOPD, recoge en su artículo 95 la figura de Responsable de Seguridad, cuya designación es obligatoria en caso de tratamiento de ficheros de nivel medio/alto. Sus funciones se centran en coordinar la implementación de las medidas de seguridad establecidas en el mencionado RLOPD.

Normativa aplicable en 2018 (RGPD): Se introduce la nueva figura del Data Protection Officer o Delegado de Protección de Datos, que asume nuevas y cualificadas competencias en materia de coordinación y control del cumplimiento de la normativa de protección de datos

Funciones del DPO

- Informar y asesorar al responsable del tratamiento de datos de las obligaciones que debe efectuar para cumplir con el Reglamento General. Debe dejar constancia en papel de las comunicaciones con el responsable del tratamiento y sus respuestas.
- Supervisar la aplicación de las normas por el encargado del tratamiento en materia de protección de datos personales. Dentro de este apartado se incluyen: asignación de responsabilidades, formación del personal y auditorías correspondientes.
- Supervisar la documentación, notificación y comunicación de las violaciones de datos personales.
- Supervisar la respuesta a las solicitudes de la autoridad de control y cooperar con ella por solicitud de las mismas o por iniciativa propia.
- Ejercer de punto de contacto con la autoridad de control sobre cuestiones relacionadas con el tratamiento de datos personales.

Funciones del DPO

Dicha figura será obligatoria cuando:

- El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
- Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de datos a gran escala; o
- Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas o infracciones penales.

LAS RELACIONES ENTRE RESPONSABLES DEL TRATAMIENTO

Regulación entre responsables

Se debe documentar de forma precisa las instrucciones respecto del encargo realizado. Es necesario identificar de forma clara y concreta cuáles son los tratamientos de datos a realizar por el encargado del tratamiento, atendiendo al tipo de servicio prestado y a la forma de prestarlo. Es especialmente necesario determinar de forma clara las comunicaciones a terceros que el responsable encomienda al encargado o que se derivan del servicio prestado.

Que tengo que hacer para cumplir?

Nuevo RGPD

Cambios en las obligaciones de las correduría

✓ Cambio en la documentación:

- La documentación que la correduría debe de tener a disposición de la Agencia Española de Protección de Datos cambia completamente, dato que ya no existirá un documento estándar de seguridad, sino que obligatoriamente se deberá de realizar un análisis de riesgos de datos y dependiendo de este se establecerán procesos y medidas de seguridad. (la documentación actual no sirve)

✓ Obtención del consentimiento inequívoco:

- El consentimiento tácito ya no es válido, por lo que habrá que tener recopilada la autorización de todos los clientes o posibles clientes, bien mediante su firma o mediante una acción positiva..

✓ Figura del delegado de protección de datos:

- La legislación establece que, dependiendo de la calidad, cantidad y finalidades de la información tratada se deberá designar un DPD, cuya figura se recomienda externa, y que sus funciones serán la supervisión del tratamiento de los datos y la mediación en conflicto y punto de contacto con la Agencia de Protección de Datos.

✓ Comunicación de incidencias:

- Otra de las novedades relevantes, es la existencia de comunicacion a la AGPD, de forma telemática, de cualquier incidencia relacionada con la protección de datos en un plazo no superior a las 72 horas.

✓ Formación:

- La legislación establece la realización de cursos de formación y concienciación en protección de datos para los empleados y colaboradores de las correduría.

Obligaciones del RGPD

Áreas de cumplimiento de la protección de datos

Análisis de riesgo

Desarrollamos el análisis de riesgo adaptado a cada una de las actividades de la empresa

DPO

Servicio de Delegado de Proteccion de Datos para asociaciones, colegios profesionales, corredurias o empresas de cualquier actividad.

DataCon

Plataforma para la recogida del consentimiento de usuarios y clientes

Formación

Parte fundamental entre las medidas a adoptar para la mitigación de los riesgos relacionados con los datos.