

De Lorenzo
A B O G A D O S

SERVICIOS INTEGRALES EN EL ÁMBITO SANITARIO

REGLAMENTO EUROPEO
DE PROTECCIÓN DE DATOS



ÁREA NUEVAS TECNOLOGÍAS

REGLAMENTO EUROPEO DE PROTECCION DE DATOS

EL BUFETE DE LORENZO ABOGADOS fue fundado en 1955 como primera Firma legal dedicada al Derecho Sanitario de forma especializada e integral, comprendiendo los sectores médico, odontológico, farmacéutico, veterinario y de enfermería, abarcando en cada uno de ellos tanto las relaciones con la Administración, como los litigios entre particulares.

DE LORENZO ABOGADOS con su estructura y dimensión, propia de "boutique legal", es hoy indiscutiblemente, el primer Despacho, por dedicación y por la importancia de sus clientes, en el área del Derecho de la Salud, y se encuentra firmemente asentado en el sector, proporcionando asesoramiento a corporaciones, a entidades y a particulares, desde sus Áreas Contenciosa, de Derecho Público, Laboral y de la Seguridad Social, Nuevas Tecnologías, Derecho Farmacéutico, Biomedicina y Biotecnología, así como Socio Sanitaria.

El Bufete ha alcanzado prestigio nacional mediante la aplicación rigurosa de sistemas y métodos de trabajo basados en un conocimiento profundo del sector, en la experiencia de los profesionales que componen la Firma, y en su exigente preparación científica, puesta de manifiesto en numerosas publicaciones y actividades docentes.

El Área de Nuevas Tecnologías en **DE LORENZO ABOGADOS** atiende de forma eficaz y especializada, las necesidades generadas como consecuencia de la evolución de la sociedad de la información, teniendo en cuenta la rapidez con la que se producen los cambios en esta materia y las consiguientes modificaciones legislativas cuyo objeto reside en la salvaguarda de los derechos de los ciudadanos, así como la incidencia que estos cambios pueden tener en el sector sanitario, como es el caso del nuevo **REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS**.

ADECUACIÓN AL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS: LA CULTURA DE LA PRIVACIDAD

El nuevo Reglamento Europeo de Protección de Datos (RGPD o GDPR por sus siglas en inglés) pretende que todas las organizaciones que tratan datos de ciudadanos europeos, sean locales o internacionales, se atiendan con una única legislación en toda la Unión Europea, evitando así diferencias de criterios y regímenes sancionadores fragmentados y desiguales.

El Reglamento proclama modernizar y dar respuesta a un mundo tecnológico en constante y rápido progreso, armonizando las normativas de todos los países de la Unión Europea y protegiendo y reforzando los derechos de los titulares de sus datos frente al ratamiento masivo de datos que realizan los responsables de los tratamientos.

Con el RGPD, la protección de los datos personales se convierte en algo más que un cumplimiento formal de obligaciones legales, tal y como venía establecido en el Reglamento español que desarrolla la Ley Orgánica de Protección de Datos. Este nuevo modelo anglosajón, pretende propiciar una verdadera cultura de la privacidad.

Figuras como el Responsable del Tratamiento, Responsable de Seguridad o el Delegado de Protección de Datos recobran sentido con este marco más sólido y coherente, regulador de un derecho fundamental, el de la protección de datos, consagrado en la Constitución Española.



PERIODO DE TRANSICIÓN: DE LA LOPD AL RGPD

El RGPD se publicó en el Diario Oficial de la Unión Europea el 4 de mayo de 2016, entrando en vigor a los 20 días de su publicación y será aplicable a partir del 25 de mayo de 2018. En este periodo transitorio, aunque sigue vigente la Ley Orgánica de Protección de Datos (LOPD), los responsables y encargados de tratamiento deben ir adaptando las medidas necesarias para cumplir la nueva normativa en el momento de su aplicación.

El RGPD es directamente aplicable y no requiere de normas internas de transposición, aunque sí permite, de forma restrictiva, su desarrollo por normas internas. Por ello, los responsables y encargados deben asumir que la norma de referencia es el RGPD con independencia de la normativa nacional.

El RGPD contiene muchos conceptos similares a los establecidos en la LOPD, sin embargo contiene nuevas obligaciones que deben ser aplicadas por cada organización, especialmente el de responsabilidad proactiva imputable a ésta o el de la prevención del riesgo de pérdida, mediante la elaboración de informes de evaluaciones de impacto.

El RGPD es de obligado cumplimiento para cualquier persona física o jurídica, autoridad pública, servicio u organismo que, solo o por encargo, realice un tratamiento de datos personales de ciudadanos residentes en la Unión Europea, independientemente que el responsable se encuentre o no dentro del territorio europeo.

NOVEDADES QUE TRAE CONSIGO EL RGPD

Cláusulas de Protección de Datos

La información debe ser más clara y detallada en base a finalidades concretas y diferenciadas (asistencia sanitaria, publicidad, etc.). Se podrá informar por capas, incluso utilizando iconos comprensibles. Además de la información exigida por la LOPD, se deberá informar sobre:

1. Los datos de contacto del Delegado de Protección de Datos, en su caso.
2. La base jurídica o legitimación para el tratamiento.
3. El plazo o los criterios de conservación de la información.
4. La existencia de decisiones automatizadas o elaboración de perfiles.
5. La previsión de transferencias a Terceros Países.
6. Los nuevos derechos del RGPD (portabilidad, limitación, reclamar ante la Autoridad de Control).

Consentimiento del titular de los datos

1. El consentimiento será siempre explícito (no cabe el consentimiento tácito, por inacción, casillas marcadas o en sentido negativo).
2. Se deberá probar que se informó adecuadamente y se obtuvo el consentimiento.
3. Se deberá permitir la revocación inmediata del consentimiento.
4. El RGPD actualiza la minoría de edad para consentir y ejercitar derechos.

Responsabilidad proactiva de la organización

1. La organización debe implicarse y ser parte activa en la implantación de un proyecto de seguridad en sus instalaciones.
2. Debe decidir qué medidas de seguridad se deben aplicar en función de la sensibilidad de la información.
3. Debe analizar los riesgos y dar soluciones en supuestos de pérdida, sustracción, o accesos indebidos de datos.
4. Deberá demostrar en todo momento la debida diligencia en el cumplimiento del RGPD.

Tratamiento de Datos Salud

1. El concepto de dato de salud se amplía incluyendo los datos biométricos y datos genéticos.
2. Se habilitan mecanismos de seguridad (la seudonimización de datos en investigación científica).
3. Quedan regulados los tratamientos de salud "a gran escala" y se actualiza la legislación a las nuevas tecnologías aplicadas al sector salud.
4. Surgen nuevos mecanismos de certificación y Códigos de Conducta al objeto de facilitar el cumplimiento a las organizaciones.

Nuevos procedimientos

1. Notificación de Violaciones de Seguridad, tanto a la Autoridad de Control como al perjudicado.
2. Ejercicio del derecho a la supresión o al olvido, o el derecho a desindexar información personal de los buscadores.
3. Nuevo procedimiento sancionatorio con un incremento de hasta 20 millones de euros o el 4% de la facturación anual de la organización.
4. Realización de Evaluaciones de Impacto (EIPD o PIA por sus siglas en inglés).
5. Se suprime la obligación de notificar ficheros ante la Agencia Española de Protección de Datos (AEPD).
6. Realización del Registro de Actividades.
7. Análisis de nuevos proyectos antes de la recogida de datos, durante su tratamiento hasta su conservación y accesibilidad (Protección de Datos desde el diseño y por defecto).
8. Designación del Delegado de Protección de Datos (DPD o DPO por sus siglas en inglés). Dicha designación será obligatoria para centros sanitarios que traten datos conforme a la Ley de Autonomía del Paciente.





PERIODO DE ADAPTACIÓN

El RGPD propone una nueva cultura de privacidad por lo que toda organización debe tener en cuenta que:

- > Se debe estar cumpliendo con la normativa española ya existente. De esta manera la transición al RGPD es mucho más rápida y sencilla.
- > Se debe regularizar las relaciones con los encargados del tratamiento, redactando los nuevos contratos que contemplen las obligaciones expuestas en RGPD o las informadas por Autoridad de Control (Directrices y/o Guías).
- > Se debe revisar el clausulado y los consentimientos ya obtenidos, determinando la necesidad o no de recopilarlos nuevamente en base a los nuevos principios de transparencia e información.
- > Se debe Implementar medidas de seguridad antes, durante y después del tratamiento de datos y siempre acordes a las necesidades y posibilidades de la organización.
- > Se debe preparar los procedimientos de atención de los nuevos Derechos en materia de protección de datos.
- > Se debe analizar los riesgos que atañen al tratamiento de datos, reconfigurándose como parte activa en la protección y asumiendo que la normativa de protección de datos es mucho más que un cumplimiento formal y/o documental.

SERVICIO DE ADECUACIÓN AL RGPD EN DE LORENZO ABOGADOS

Desde **DE LORENZO ABOGADOS** ofrecemos asesoramiento legal en materia de cumplimiento del RGPD, enfocada a empresas y entidades del sector sanitario, aplicando nuestro conocimiento de este sector, así como nuestra dilatada experiencia en el mismo.

Ayudando a empresas y organizaciones del sector para superar los retos a los que se enfrentan dando una respuesta eficaz y acorde a las disciplinas implicadas.

DE LORENZO ABOGADOS define los objetivos de adecuación en base a los siguientes criterios:

- > Redacción de los nuevos clausulados y contratos conforme al Reglamento General de Protección de Datos y las Directrices de la Autoridad de Control.
- > Elaboración del registro de actividades.
- > Aproximación basada en el Riesgo. Preparación de las Evaluaciones de Impacto (EIPD).
- > Implantación de medidas de seguridad adecuadas para la organización. Protección de Datos y Prevención del Riesgo (Privacidad desde el diseño y por defecto).
- > Preparación del nuevo procedimiento de notificación de violaciones de seguridad, tanto a la Autoridad de Control como al propio afectado.
- > Regulación en materia de transferencias internacionales de datos.
- > Redacción de los nuevos procedimientos de atención de los Derechos que expone el Reglamento.
- > Designación de la figura del Delegado de Protección de Datos (DPD). Podrá ser personal interno o externo a la organización pero, en todo caso, deberá ser designado atendiendo a sus cualidades profesionales y en particular a sus conocimientos especializados en Derecho. Sus cometidos son los de informar y asesorar a los responsables y encargados respecto del cumplimiento del RGPD y sus nuevos procedimientos así como de las normativas sectoriales específicas aplicables a cada organización. Supervisará el cumplimiento del RGPD y atenderá a los ciudadanos respecto de sus derechos debiendo cooperar en todo momento con la Autoridad de Control (consulta previa, conflictos, etc.).
- > Concienciación y formación al personal en materia del nuevo Reglamento así como de su principio de responsabilidad proactiva mediante cursos de formación y/o charlas departamentales.
- > Consultoría externa (asesoramiento en materia del RGPD).

En base a lo anterior, **DE LORENZO ABOGADOS** proporciona la documentación que se lista a continuación relativa a los siguientes bloques:

Entregables:

- > Delegado de Protección de Datos, preparación de documentos de formalización del nombramiento del DPD así como las relativas a las actas de reuniones.
- > Política de evidencias de cumplimiento.
- > Registro de actividades del tratamiento.
- > Cláusulas de información actualizadas y de obtención del consentimiento para todas las áreas de la organización (bases de datos de Historias Clínicas, datos biométricos, videovigilancia, datos del personal, etc..)
- > Contratos de encargado del tratamiento, de cesión de datos y sin permiso de acceso a la información conforme a las directrices de la Autoridad de Control.
- > Cláusulas de confidencialidad para terceros.
- > Protocolo de tutelas de derechos actualizados.
- > Propuesta de controles periódicos de cumplimiento.
- > Procedimiento de gestión de brechas de seguridad.
- > Documentación de la metodología para la elaboración de Evaluaciones de Impacto para la Privacidad.

delorenzoabogados.es

MADRID

Velázquez, 124
28006 Madrid

Tels: +34 91 561 17 12
+34 91 561 01 78
Fax: +34 91 411 41 07
firm@delorenzoabogados.es

VALENCIA

EDIFICIO SAMANIEGO
Samaniego, 6 (esquina c/ Navello)
46003 Valencia

Tels: +34 96 315 31 94
Fax: +34 91 411 41 07
valencia@delorenzoabogados.es

ruervas