etiqampus
e-Learning en Integridad

# Guía Comparada Protección de Datos Personales: caso España

Compliance Internacional

NIVEL INTERMEDIO

| | |
|---|---|
| **Fecha** | Marzo 2025 |
| **Tpo. de lectura** | 23 min. |

El avance tecnológico y la transformación digital han puesto la protección de datos personales en el centro del debate regulatorio a nivel global. En Latinoamérica, el desarrollo y fortalecimiento de normativas en esta materia reflejan la creciente necesidad de garantizar la privacidad y seguridad de la información en un entorno empresarial cada vez másbinterconectado.

La evolución de estas regulaciones y su aplicación práctica imponen nuevos desafíos a las organizaciones, que deben adaptar sus procesos y modelos de negocios para cumplir con estándares más altos y responder a las exigencias de las autoridades regulatorias y fiscalizadoras.

En este contexto, especialista de destacadas firmas legales de 18 países miembros de Compliance Latam, han elaborado esta guía que, además de dar una visión clara y actualizada sobre los marcos normativos y últimas tendencias en protección de datos personales, entrega herramientas clave para que las empresas comprendan y gestionen los riesgos asociados al tratamiento de datos, fomenten una cultura de cumplimiento y refuercen la confianza con sus clientes y socios comerciales.

A continuación te presentamos la sección dedicada a España, escrita por Florencia Arrébola, Asociada Senior, Propiedad Intelectual, Media, Corporativo del estudio Bartolomé y Briones.

FGE

az albagli zaliasnik

BARTOLOME & BRIONES

Com plian ce LATAM

FUENTE: el texto de esta portadilla se elaboró a partir de la introducción de la “Guía Comparada Protección de Datos Personales” publicada por la plataforma “Compliance Latam”.

# Guía Comparada Protección de Datos Personales

Marzo 2025



www.compliancelatam.legal



BARTOLOME & BRIONES

Autor:

**Florencia Arrébola,** Asociada Senior, Propiedad Intelectual, Media, Corporativo.

**1. ¿Cuál es el marco regulatorio de la protección de datos personales en tu jurisdicción?**

En España, la protección de datos personales está regulada principalmente por el Reglamento General de Protección de Datos (RGPD), que es una normativa de la Unión Europea aplicable a todos los Estados miembros. Este reglamento establece un marco armonizado para la protección de datos personales, asegurando derechos a los individuos y obligaciones a los responsables del tratamiento. El RGPD destaca principios como la responsabilidad proactiva, licitud, lealtad y transparencia, la limitación de la finalidad y la minimización de datos, que deben ser observados por cualquier entidad que maneje datos personales.

Además, la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) complementa y desarrolla el RGPD en el contexto español. Ambas normativas se fundamentan en principios esenciales de protección de datos, que no solo buscan salvaguardar la privacidad de los individuos, sino también fomentar la confianza en el uso de tecnologías digitales.

**2. ¿Existe en tu país regulación sobre programas de prevención de infracciones o de cumplimiento en materia de protección de datos personales? ¿Son obligatorios? ¿En qué casos?**

Sí, tanto el RGPD como la LOPDGDD establecen la obligación a los responsables y encargados del tratamiento de implementar medidas de cumplimiento en materia de protección de datos que se aplicarán atendiendo a la naturaleza, contexto, finalidad del tratamiento y los riesgos que el tratamiento de datos pueda implicar para los derechos y libertades de los ciudadanos. Estas medidas deben aplicarse desde el diseño y por defecto, es decir que deben tenerse en consideración desde el nacimiento y diseño de un proceso que implica el tratamiento de datos personales. En concreto, el artículo 24 del RGPD y el artículo 28 de la LOPDGDD exigen que los responsables adopten medidas técnicas y organizativas apropiadas. En este sentido, el principio de responsabilidad proactiva implica que cada responsable de tratamiento de datos deberá analizar y valorar cuáles son las medidas técnicas y organizativas que deben adoptarse en cada circunstancia para demostrar que se cumple con las obligaciones de la normativa frente a las autoridades de control y supervisión competentes.

Estas medidas pueden implicar no solo la creación de políticas y procedimientos internos, sino también la implementación de tecnologías adecuadas para proteger los datos. Por ejemplo, entre las medidas técnicas comúnmente utilizadas encontramos el uso de contraseñas seguras, actualización de los sistemas y copias de seguridad, y entre las medias organizativas destacamos la aplicación de políticas de privacidad, formación del personal, controles de acceso a la información y desarrollar auditorias regulares.

Por otro lado, el artículo 32 del RGPD describe las medidas de seguridad que se deben adoptar y enumera entre otras, técnicas como la seudonimización y cifrado de datos, garantizar la confidencialidad, integridad, disponibilidad y resiliencia de sistemas y servicios de tratamiento, capacidad para restaurar la disponibilidad y el acceso a los datos.

**3. ¿Qué contenido mínimo deben tener los programas de cumplimiento en protección de datos personales en tu país?**

Como mencionamos en la respuesta anterior, si bien la normativa no determina las características de las medidas técnicas y organizativas que las organizaciones pueden adoptar, en la práctica, dichas medidas se caracterizan por los siguientes elementos:

**Medidas técnicas:**

• Uso de contraseñas seguras, para garantizar la seguridad del acceso a los sistemas e información de la organización.

• Actualización de los sistemas, a fin de que éstos sean más seguros frente a posibles amenazas externas.

• Copias de seguridad periódicas que permitan garantizar la recuperación de los datos en caso de que éstos sean eliminados o resulten dañados.

**Medidas organizativas:**

• Políticas de privacidad y protección de datos: documentos claros que informen a los empleados y a los interesados sobre cómo se manejan sus datos.

• Formación continua del personal sobre obligaciones en materia de protección de datos: en concreto se podrán llevar a cabo la capacitación regular para asegurar que todos los empleados conocen sus responsabilidades en el manejo de datos personales.

• Controles de acceso a la información: limitar el acceso a la información de manera que cuantas menos personas

tengan acceso a la información menor será el riesgo de que los datos personales se comprometan.

• Mecanismos de supervisión y auditoría interna: se basa en el desarrollo de herramientas para evaluar la efectividad de las políticas y detectar posibles fallos en el cumplimiento.

**4. ¿Qué beneficios trae contar al interior de la organización con un programa de cumplimiento en protección de datos personales?**

La adopción de las medidas técnicas y organizativas apropiadas ofrece beneficios significativos, tales como:

• Reducción de riesgos de incumplimiento y sanciones administrativas: un programa efectivo ayuda a identificar y mitigar riesgos potenciales, evitando así sanciones que pueden ser económicas y reputacionales.

• Mejora de la reputación y confianza con los clientes y usuarios: las organizaciones que demuestran un compromiso sólido con la protección de datos pueden ganar la confianza de sus clientes, lo que puede traducirse en lealtad y un incremento en la base de clientes.

• Fomento de una cultura de responsabilidad y ética en el manejo de datos: los programas de cumplimiento contribuyen a crear un entorno laboral donde se valora la privacidad y la protección de datos.

Asimismo, el compromiso con estas medidas y su adecuación a las características del tratamiento de datos y su finalidad, servirá para demostrar que se cumple con la normativa frente a las autoridades de control y supervisión competentes.

**5. ¿Existen procesos de certificación de los programas de cumplimiento en protección de datos en tu país? ¿Quién realiza la certificación?**

Sí, existen procesos de auditoría y certificación en materia de protección de datos, los cuales son reconocidos por el RGPD. En concreto la certificación "Europrivacy" aborda las obligaciones específicas del RGPD a la vez que funciona como esquema de certificación oficial y es aplicable al tratamiento de datos que se lleva a cabo en las organizaciones permitiendo evaluar y certificar su conformidad con el RGPD y LOPDGDD.

La certificación puede ser realizada por organismos de certificación acreditados que evalúan el cumplimiento de las normas de protección de datos, ofreciendo un mecanismo para demostrar la conformidad ante las autoridades y los interesados.

**6. ¿En tu jurisdicción es obligatorio contar con un delegado de protección de datos personales? ¿En qué casos?**

El RGPD y la LOPDGDD delimitan los supuestos en los que es necesario designar un Delegado de Protección de Datos (DPO).

En este sentido, la LOPDGDD regula este aspecto de forma más detallada, estableciendo los siguientes supuestos en los que los responsables y los encargados del tratamiento deberán designar un DPO:

• Los colegios profesionales y sus consejos generales.

• Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

• Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

• Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

• Las entidades de crédito (bancos, cajas de ahorro, cooperativas de crédito, el Instituto de Crédito Oficial).

• Los establecimientos financieros de crédito.

• Las entidades aseguradoras y reaseguradoras.

• Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

• Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

• Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

• Las entidades que desarrollen actividades de

publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

• Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

• Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

• Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

• Las empresas de seguridad privada.

• Las federaciones deportivas cuando traten datos de menores de edad.

Por otro lado, el RGPD establece la obligatoriedad de designar un DPO en los siguientes supuestos:

• Cuando el tratamiento de datos lo realiza una autoridad pública, excluyendo a los tribunales actuando en función judicial.

• Si las actividades principales del responsable o encargado del tratamiento implican la observación habitual y sistemática de datos personales a gran escala.

• Cuando se trata del tratamiento a gran escala de categorías especiales de datos, como el origen étnico, opiniones políticas, datos genéticos, entre otros.

Por lo tanto, el DPO deberá designarse obligatoriamente en los supuesto sindicados y de forma voluntaria en aquellos supuestos que las organizaciones así lo consideren. Tras la designación del DPO, la decisión se debe comunicar a la Agencia Española de Protección de Datos (AEPD).

### 7. ¿Existen sanciones asociadas al incumplimiento de la normativa sobre protección de datos personales? ¿De qué tipo? ¿A cuánto ascienden las multas?

Sí, el incumplimiento del RGPD y de la LOPDGDD puede derivar en la imposición de sanciones económicas o medidas como la suspensión temporal del tratamiento de datos o la obligación de rectificar o suprimir datos.

El RGPD en primer lugar, clasifica ciertas sanciones administrativas que pueden ascender hasta 10 millones de euros o el 2% del volumen de facturación anual global (es decir, del grupo de sociedades) del responsable o encargado, y, en segundo lugar, establece sanciones económicas más gravosas para aquellas infracciones consideradas muy graves, que podrán ascender hasta 20 millones de euros, o el 4% de la facturación anual global del responsable o encargado, la que sea mayor.

Además, la normativa establece criterios para graduar el importe de las sanciones, como por ejemplo la naturaleza, gravedad y duración de la infracción, acciones adoptadas para mitigar los daños ocasionados, los beneficios económicos obtenidos, la reincidencia, la intencionalidad de la infracción, categoría de datos comprometidos, así como cualesquiera otras circunstancias relevantes para determinar la culpabilidad.

Por otro lado, la LOPDGDD determina los diferentes importes que se indican a continuación:

• Incurrir en una infracción leve puede acarrear una sanción de hasta 40.000€.

• Incurrir en una infracción grave puede acarrear una sanción de entre 40.000€ hasta 300.000€.

• Incurrir en una infracción muy grave puede acarrear una sanción a partir de 300.000.

### 8. ¿Qué tipo de conducta sanciona la normativa en protección de datos personales de tu país?

Las infracciones pueden clasificarse en leves, graves y muy graves, y las sanciones varían en función de la gravedad de la infracción.

Se consideran infracciones leves, por ejemplo, no proporcionar toda la información requerida al interesado en incumplimiento del principio de transparencia, no atender las solicitudes de ejercicios de derechos o no responder a la solicitud de supresión de los datos personales de una persona fallecida.

Tendrán la consideración de infracciones graves, por ejemplo, falta de consentimiento al tratamiento de datos personales de menores de edad, incumplimiento de medidas técnicas y organizativas necesarias o no disponer de actividades de registro de tratamiento.

Finalmente, se considerarán infracciones muy graves, por ejemplo, trata datos especialmente protegidos sin cumplir con los requisitos legales, ceder datos personales en supuestos no permitidos, realizar transferencias internacionales de datos sin contar con las garantías adecuadas, utilizar los datos personales para un finalidad incompatible con aquella para la que fueron recogidos originalmente, tratar datos personales relativos a condenas penales fuera de los supuestos permitidos, vulnerar los derechos de confidencialidad establecidos o incumplimiento de la obligación de bloqueo de los datos (previa a la eliminación de los mismos).

**9. ¿Tu jurisdicción tiene un organismo técnico que dicte directrices y fiscalice el cumplimiento de las normas de protección de datos personales?**

Sí, en España, la AEPD es el organismo encargado de supervisar y garantizar el cumplimiento de la normativa de protección de datos. La AEPD tiene la autoridad para investigar infracciones, imponer sanciones y facilitar orientación sobre la aplicación de la ley. Además, publica guías y recursos que ayudan a las organizaciones a entender sus obligaciones y a implementar prácticas adecuadas de protección de datos.

La AEPD también se encarga de promover la sensibilización sobre la importancia de la protección de datos, organizando campañas y formando alianzas con otras entidades para fomentar una cultura de privacidad en la sociedad.

**10. ¿Cuáles son los primeros pasos que toman las organizaciones en tu país para comenzar a aplicar la normativa en protección de datos personales en general y un programa de cumplimiento en particular?**

Las organizaciones suelen comenzar con una auditoría de sus prácticas de tratamiento de datos, identificando flujos de datos y evaluando riesgos asociados. Este análisis inicial es crucial para entender qué datos se manejan, cómo se procesan y quién tiene acceso a ellos. A partir de esta auditoría, las organizaciones pueden desarrollar un plan de acción para abordar las necesidades y deficiencias de cada actividad o proyecto, a fin de adoptar las medidas necesarias para cumplir con la normativa.

Además, normalmente se establecen políticas y procedimientos internos que reflejen su compromiso con la protección de datos.

**11. ¿Cuál es el ámbito de aplicación territorial de la normativa de protección de datos de tu país? ¿La normativa puede aplicarse extraterritorialmente?**

La normativa de protección de datos en España, a través del RGPD, se aplica a todas las organizaciones que procesan datos personales de individuos en la UE, independientemente de si están ubicadas dentro o fuera de la UE. Esto significa que empresas fuera de la UE que ofrezcan bienes o servicios a personas en la UE o que monitoricen su comportamiento están sujetas a las mismas obligaciones que las organizaciones dentro de la UE.

Esta aplicabilidad extraterritorial refleja el compromiso del RGPD de proteger los datos personales de los ciudadanos de la UE, asegurando que los estándares de protección se mantengan independientemente de dónde se realice el tratamiento de los datos. Esto también crea un marco de responsabilidad global para las empresas que operan en el entorno digital cada vez más interconectado de hoy.