CORDERO INFORMÁTICOS
- Informática Empresarial desde 1988 -

Paseo de la Florida 19, 3D – 28008 (Madrid)
Tfno: +34 915 500 694
Fax: +34 915 500 695
Correo: info@123cya.com
Web: https://corderoinformaticos.com

# Guía sobre la protección de los Datos Personales

**El 25 de mayo de 2018** entra en vigor el nuevo Reglamento General de Protección de Datos (RGPD / GDPR en inglés), que regula la forma en que se deben tratar los datos personales de los residentes en la Unión Europea y que establece requisitos estrictos a la hora de tratar y utilizar dichos datos.

El RGPD será de **obligado cumplimiento para todas aquellas personas, entidades u organizaciones, europeas o no, que dispongan de información personal de residentes en la Unión Europea. Su incumplimiento se sanciona con** multas considerables de **hasta el 4% de la facturación anual mundial o de 20 millones de euros**, sin contar con los inevitables **daños para la reputación**. Estas sanciones no contemplan ningún tipo de exclusión o excepción para las pequeñas empresas.

Este nuevo reglamento, junto con la creciente importancia de la digitalización y de la información en general, es el principal motivo para poner mayor énfasis en la protección de los datos personales y la privacidad de los empleados, clientes, proveedores y socios comerciales.

## ¿Qué son los datos personales?

Los datos personales pueden dividirse en dos categorías: **Datos personales** y datos personales confidenciales (“**Datos sensibles**”), que requieren protección específica.

Por Datos Personales se entiende toda aquella información relacionada con un individuo identificado o identificable, que puede ser utilizada de manera independiente o conjuntamente con otra información para contactar, ubicar o de alguna manera identificar a una persona.

Algunos ejemplos de Datos personales:

- Información de contacto (nombre, dirección, correo electrónico y número de teléfono).
- Edad, sexo y nacionalidad.
- Fecha de nacimiento, número del DNI o de la Seguridad Social y/o número de empleado.
- Información sobre el salario y el registro de horas trabajadas.
- Perfiles de usuario y registros electrónicos sobre el uso que hace un empleado de los recursos informáticos.
- Información relacionada con los hábitos de compra de una persona.
- Información sobre la ubicación de una persona.

CORDERO INFORMÁTICOS
- Informática Empresarial desde 1988 -

Paseo de la Florida 19, 3D – 28008 (Madrid)
Tfno: +34 915 500 694
Fax: +34 915 500 695
Correo: info@123cya.com
Web: https://corderoinformaticos.com

Por Datos Sensibles entendemos datos personales que requieren una protección específica, puesto que revelan opiniones políticas, origen racial o étnico, información sobre la salud, creencias religiosas o filosóficas, afiliación sindical o información sobre la vida u orientación sexual. Los datos sensibles también incluyen datos genéticos y biométricos.

También se aplican requisitos estrictos al tratamiento de datos personales relacionados con crímenes y condenas judiciales. Dicho tratamiento debe realizarse siempre siguiendo los procedimientos internos de conformidad con la legislación aplicable.

## ¿Qué es el tratamiento de datos?

Por tratamiento de datos se entiende cualquier operación que implique el uso de datos personales. Esta definición abarca la recopilación, el almacenamiento, el uso, la modificación, la eliminación, la destrucción, la estructuración, la divulgación, la transferencia, la transmisión o cualquier otra forma de tener datos personales a su disposición.

Algunos ejemplos de tratamiento de datos:

- Cuando se contrata a nuevos empleados, se necesitan datos personales de éstos. Al recopilar, registrar y usar sus datos personales, ya se están tratando datos.
- La recopilación, el registro y el uso de datos personales con fines comerciales.
- La recopilación y el uso de datos personales para ofrecer servicios de viaje a los empleados a través de una agencia de viajes.
- El uso de datos personales para crear cuentas de usuario en los sistemas informáticos.

## Principios básicos del RGPD

### Responsabilidad

Las empresas no sólo deben cumplir, sino que además deben demostrar que cumplen sus responsabilidades respecto al tratamiento de los datos: confidencialidad, seguridad, control...

### Prevención

Desde el mismo diseño del tratamiento de datos y durante todo el tratamiento de los mismos, deben adoptarse las medidas necesarias para su seguridad en función de su sensibilidad.

### Transparencia

Paseo de la Florida 19, 3D – 28008 (Madrid)
Tfno: +34 915 500 694
Fax: +34 915 500 695
Correo: info@123cya.com
Web: https://corderoinformaticos.com

Los usuarios deben ser informados de forma clara, sencilla e inequívoca, del uso que se está dando a sus datos, garantizando en todo momento sus derechos sobre los mismos.

## Normas básicas del RGPD

### Protección de Datos

Conlleva respetar los derechos de las personas a la privacidad y garantizar que no se hace un uso indebido y/o abusivo de sus datos personales.

Se pueden recopilar, utilizar o tratar datos personales sólo para fines específicos, explícitos y legítimos, justificados de forma objetiva. **No se deben recopilar más datos personales de los que se necesitan para cumplir el objetivo del tratamiento.** Una vez que los datos personales dejen de ser necesarios para el propósito del tratamiento, deben eliminarse o hacerse anónimos. Nunca pueden ser usados de modo incompatible con el propósito original.

Por ejemplo:

Si tiene acceso a sistemas de TI que muestren los registros de actividad de un empleado, no debe consultar la información de sus colegas haciendo uso del acceso del que dispone en interés personal o para un fin distinto del original.

**Se debe asegurar la calidad y exactitud de los datos personales, así como su permanente actualización. Deben existir mecanismos para corregir cualquier inexactitud o incluso para suprimirlos en el menor plazo posible.**

Se debe realizar el tratamiento de datos garantizando la seguridad de los mismos y tomando las medidas adecuadas para proteger los datos personales y evitar un uso incorrecto, pérdida, divulgación o acceso no autorizado a éstos, cumpliendo con las obligaciones de confidencialidad.

### Tratamiento lícito

Sólo es lícito el tratamiento de los datos cuando el interesado da su consentimiento **libre, inequívoco y explícito**; cuando es necesario para la firma de un contrato, por obligación legal o interés público o para proteger intereses legítimos, salvo que prevalezcan los propios del interesado.

El uso de los datos debe cumplir con los principios de **licitud, lealtad, transparencia, caducidad, proporcionalidad, integridad y confidencialidad** establecidos.

Algunos ejemplos de finalidad legítima a la hora de tratar datos personales:

Paseo de la Florida 19, 3D – 28008 (Madrid)
Tfno: +34 915 500 694
Fax: +34 915 500 695
Correo: info@123cya.com
Web: https://corderoinformaticos.com

- Recursos humanos y gestión interna o del personal.
- Salud, seguridad e integridad, incluida la gestión de manejo de crisis y la salvaguarda de la seguridad e integridad del sector empresarial en el que opera la empresa.
- Ejecución y cierre de acuerdos con clientes, proveedores y socios comerciales.
- Ejecución del servicio de atención al cliente.

### Transferencias de datos internacionales

Se mantiene la prohibición, salvo en casos especiales, de enviar datos personales a países fuera de la Unión Europea que no tienen una protección adecuada.

## Principales novedades del RGPD

### Derechos de los usuarios

La información a los usuarios sobre los derechos y tratamientos que les afecten deberá presentárseles de forma clara y sencilla. Entre otras novedades, destacamos las siguientes:

- El derecho al olvido.
- El derecho de portabilidad.

### Consentimiento explícito

Se requiere una acción afirmativa clara por parte del usuario para confirmar su consentimiento para la recogida de datos. No son válidas las acciones por omisión ni se puede extrapolar a otros tratamientos distintos el consentimiento dado a un tratamiento, necesitándose consentimientos independientes para cada uno de los tratamientos. La retirada del consentimiento debe ser tan fácil como su concesión.

### Ámbito de aplicación del RGPD

Las violaciones del reglamento no sólo afectan a la entidad que recoge los datos, sino también a cualquier tercero que los procesa en su nombre.

Además, no sólo se aplica en la Unión Europea, sino que afecta a cualquier organización o entidad que haga tratamiento de datos de ciudadanos de la Unión Europea.

Las instituciones benéficas y las ONG se encuentran sujetas también al RGPD.

### Responsabilidad proactiva

Paseo de la Florida 19, 3D – 28008 (Madrid)
Tfno: +34 915 500 694
Fax: +34 915 500 695
Correo: info@123cya.com
Web: https://corderoinformaticos.com

Según este principio, se deberán realizar análisis de riesgo de distinta profundidad según el tamaño de la empresa y la sensibilidad de los datos. Algunas empresas y organizaciones deberán mantener registros sobre la obtención de los consentimientos, las actividades de tratamiento, las incidencias de seguridad…

El concepto de "protección de datos desde el diseño y por defecto" se refiere a plantear medidas para la protección de los datos desde el mismo momento en que se diseña un tratamiento y durante toda la vida del mismo.

Cualquier violación del RGPD debe notificarse a las autoridades de control en un plazo máximo de 72 horas y, si entraña grave riesgo para el interesado, debe notificársele también a él sin dilación. Esta notificación al interesado no sería necesaria **si los datos estuviesen protegidos con anterioridad a la vulneración de seguridad mediante medidas como el cifrado, que los hacen ininteligibles para terceros.**

La figura del Delegado de Protección de Datos, con conocimientos jurídicos y técnicos sobre la protección de datos, será obligatoria en autoridades y organismos públicos y en organizaciones que realicen tratamientos que requieran observación habitual y sistemática de interesados a gran escala o tratamientos a gran escala de datos sensibles.

## Evaluación y medidas

**Son las propias empresas las que deberán evaluar la sensibilidad de sus datos y decidir qué medidas adoptar para su correcto tratamiento** y deberán seguir sin excepción los siguientes pasos:

### 1. Análisis de impacto sobre la Privacidad

Evaluación mediante auditoría de datos de la sensibilidad de los mismos y los riesgos para la privacidad. Con los resultados de la auditoría se acreditará ante la AEPD los datos que se van a recoger y el uso que se les va a dar, los datos del responsable del tratamiento y las pruebas temporales que van a garantizar la seguridad.

### 2. Documentación de los procesos

Todos los procesos relacionados con el tratamiento de los datos (gestión, acceso, recolección...) deberán ser documentados y adecuados a los resultados del análisis de riesgo realizado con las medidas de seguridad pertinentes.

### 3. Formación del personal

Paseo de la Florida 19, 3D – 28008 (Madrid)
Tfno: +34 915 500 694
Fax: +34 915 500 695
Correo: info@123cya.com
Web: https://corderoinformaticos.com

Todo el personal interno relacionado por contrato con el tratamiento de los datos deberá recibir formación sobre el mismo y sobre la seguridad de los datos.

### 4. Contratos con terceros

Antes de dar acceso a los datos a cualquier tercero, hay que firmar acuerdos de confidencialidad y exigirles sus propias auditorías de seguridad.

### 5. Delegado de Protección de Datos (*)

Se debe designar un delegado, interno o externo, que supervise la correcta aplicación del reglamento y sirva de enlace con los organismos oficiales.

**Sólo empresas de más de 250 empleados o de menor tamaño que traten datos sensibles*

### 6. Notificación de violaciones de seguridad

Existe la obligación de detectar las violaciones de seguridad y de notificarlas a la AEPD y al interesado, en caso de riesgo para el mismo.

**ESENCIA FUNDAMENTAL DEL RGPD**

Se debe realizar el tratamiento de datos con **la mejor opción para mitigar el riesgo** tomando las medidas adecuadas para proteger los datos personales y evitar un uso incorrecto, pérdida, divulgación o acceso no autorizado a éstos, cumpliendo con las obligaciones de confidencialidad. El RGPD pone la responsabilidad en **la prevención**, de forma que una empresa será culpable **únicamente** cuando no haya puestos los medios que considere oportunos para proteger sus datos.

## ¿Dónde encuentro más información?

- http://www.agpd.es/portalwebAGPD/temas/reglamento/index-ides-idphp.php
- https://www.eugdpr.org

## ¿Cómo podemos desde Cordero y Asociados ayudarle?

Como empresa de servicios informáticos desde 1988, estamos al día de las tecnologías y trabajamos con los principales protagonistas del sector para ayudar a nuestros clientes a tener sus datos protegidos y cumplir con las leyes, por lo que ofrecemos los siguientes servicios:

- Análisis de riesgos de accesos físicos a la empresa, a la sala de servidores y equipos en general.

Paseo de la Florida 19, 3D – 28008 (Madrid)
Tfno: +34 915 500 694
Fax: +34 915 500 695
Correo: info@123cya.com
Web: https://corderoinformaticos.com

- Análisis de riesgos de seguridad lógica que incluye entre otras:
- Inventario de dispositivos autorizados y No autorizados.
- Inventario de Software autorizado y No autorizado.
- Configuración segura del Hardware y Software en dispositivos Móviles, portátiles, estaciones de Trabajo y servidores.
- Evaluación de vulnerabilidades y correcciones continuas.
- Uso controlado de privilegios administrativos.
- Mantenimiento, supervisión y análisis de registros de auditorías.
- Protecciones de correo electrónico y explorador web.
- Protecciones contra virus y malware.
- Limitación y control de los puertos de Red, protocolos y servicios.
- Copias de seguridad y capacidad de recuperación de Datos.
- Configuraciones seguras para dispositivos de Red como firewalls, routers y switches.
- Control de acceso inalámbrico.
- Supervisión y control de cuentas.
- Evaluación y formación a los empleados sobre habilidades de seguridad.
- Seguridad de Software de aplicación.
- Gestión y respuesta ante incidentes.

Documentación para el cumplimiento del RGPD que incluye informe sobre lo realizado, mejoras a hacer, ejecución de las mejoras, registro de incidencias, mantenimiento y declaración de las incidencias si las hubiera a los afectados y a la agencia de protección de datos.