



Bienvenido al curso de

Fundamentos de la protección de datos personales

El objetivo de este curso es difundir y enseñar los conceptos básicos del nuevo Reglamento de Protección de Datos, que afecta a todos los trabajadores, colaboradores y usuarios en el desarrollo de sus funciones laborales y profesionales.

La normativa de protección de datos obliga a las empresas y organizaciones a velar por su efectivo cumplimiento, lo que implica la obligación de poner en conocimiento de todos sus usuarios las nociones básicas para que traten los datos adecuadamente y que conozcan cuáles son sus funciones y obligaciones en el tratamiento de los mismos.

Cuando finalice de este curso, en definitiva, como usuario que trata o puede tratar datos personales responsabilidad de la empresa, deberá haber aprendido:

- Qué son y cómo tratar los datos personales
- Las obligaciones impuestas por el Reglamento
- Los procedimientos y protocolos de cumplimiento del Reglamento.

¿Qué es un dato personal?



Un dato personal es “toda información sobre una persona física identificada o identifiable”, es decir, cualquier dato que permita, sin esfuerzos desproporcionados, determinar, directa o indirectamente, la identidad de una persona física.

Ejemplos:

- Nombre y apellidos
- Dirección, teléfono, correo electrónico
- Fecha y lugar de nacimiento
- DNI, Pasaporte, etc.
- Imagen
- Datos de salud
- Etc.

¿Por qué se protegen?

La protección de los datos personales es un **Derecho Fundamental** recogido en Carta de los Derechos Fundamentales de la Unión Europea y en la Constitución Española, que poseen todos los ciudadanos, consistente en que sus datos de carácter personal no sean utilizados por terceros sin contar con su debido consentimiento.

La norma que regula el tratamiento de datos de carácter personal es el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.



En principio,
los datos
personales sólo
pueden
utilizarse con el
consentimiento
del titular

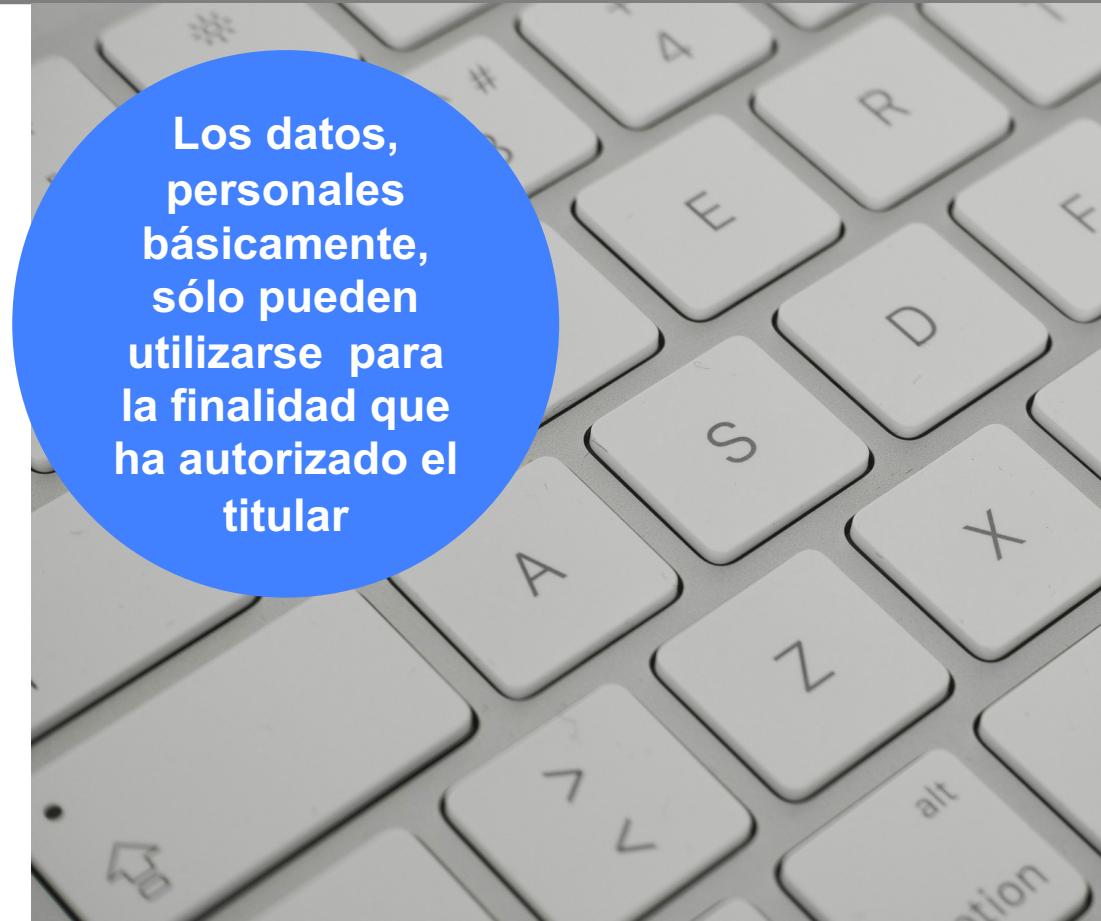
1.- Introducción a la Protección de Datos Personales

Tratamiento de datos y Responsables

Tratamiento de datos es cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados (ordenador) o no (en papel).

El tratamiento de datos personales tiene tres fases:

- Solicitud: incorporación a los ficheros.
- Tratamiento: utilización y conservación de los datos.
- Supresión: fin de tratamiento de los datos.



Los datos, personales básicamente, sólo pueden utilizarse para la finalidad que ha autorizado el titular

1.- Introducción a la Protección de Datos Personales

Responsables



Cualquier empresa u organización es responsable de los datos que le han facilitado los titulares

Responsable del tratamiento o “Responsable” es la persona física o jurídica, autoridad, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Ejemplos de Responsables:

Universidades, Colegios, Bancos, Hospitales, Comercios, Gimnasios, Bibliotecas, Administraciones públicas, Asociaciones, Comunidades de propietarios y, en definitiva, cualquier organización que disponga de trabajadores o clientes.

Clasificación de los datos y nivel de seguridad

El Reglamento no establece niveles de riesgo pre establecidos como antes (básico, medio y alto) y es necesario valorar el tratamiento que realiza cada responsable.

Las medidas de seguridad se aplicarán en base a una valoración del riesgo inicial, a la que debe someterse cualquier entidad responsable de tratamiento de datos personales, y que básicamente tiene en consideración:

- El tipo de datos (si son sensibles o no)
- La cantidad de datos tratados
- El ámbito geográfico
- La frecuencia del tratamiento de esos datos
- La duración del tratamiento.

Todo responsable debe valorar el riesgo del tratamiento



1.- Introducción a la Protección de Datos Personales



Las autoridades de protección de datos son el Comité Europeo de Protección de Datos, la Agencia Española de Protección de Datos y, donde existan, las Agencias Autonómicas de Protección de Datos.

Sus funciones son: velar por el cumplimiento de la legislación; la salvaguarda y tutela de los derechos de los ciudadanos; función consultiva e informativa; cooperación con otras autoridades; el control y cooperación internacional; la inspección y la potestad sancionadora.

Cualquier ciudadano puede dirigirse a ella para denunciar la vulneración de sus derechos.

1.- Introducción a la Protección de Datos Personales

Principios Básicos del Reglamento



Los Principios Básicos del RGPD son:

- Licitud, lealtad y transparencia.
- Limitación de la finalidad.
- Minimización de datos.
- Exactitud.
- Limitación del plazo de conservación.
- Integridad y confidencialidad.
- Responsabilidad proactiva.

2.- Principios, Obligaciones y Exigencias del Reglamento de Protección de Datos

Consentimiento



Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

Ejemplos:

- Para enviar publicidad
- Para utilizar la imagen
- Para ceder los datos
- Etc.

2.- Principios, Obligaciones y Exigencias del Reglamento de Protección de Datos

Categorías especiales de datos

Son categorías especiales de datos:

- el origen étnico o racial;
- las opiniones políticas, convicciones religiosas o filosóficas;
- la afiliación sindical;
- los datos genéticos;
- los datos biométricos dirigidos a identificar de manera unívoca a una persona física;
- los datos relativos a la salud;
- y los datos relativos a la vida sexual o la orientación sexual de una persona física.

El Reglamento prohíbe el tratamiento de datos de categorías especiales si no ha habido consentimiento, salvo algunas excepciones que determina.



2.- Principios, Obligaciones y Exigencias del Reglamento de Protección de Datos

Deber de Secreto y Derecho de Información

El deber de secreto es un derecho fundamental que asegura que los datos personales sólo sean conocidos por el interesado y por aquellos usuarios de la organización que requieren acceder a ellos para el desarrollo de sus funciones laborales.

El derecho de información en la solicitud de datos personales es el que disponemos todos los ciudadanos de que se nos informe previamente sobre el tratamiento de nuestros datos.

Esta información debe ser concisa, transparente, inteligible, de fácil acceso y con un lenguaje claro y sencillo.



Los titulares
tienen
derecho a ser
informados y
sus datos
deben ser
secretos

2.- Principios, Obligaciones y Exigencias del Reglamento de Protección de Datos

El principio de calidad y la Comunicación de Datos



El principio de calidad de los datos contiene los siguientes principios:

- Limitación de la finalidad.
- Minimización de datos.
- Exactitud.
- Limitación del plazo de conservación.

Sólo se pueden comunicar datos a terceros:

- con el consentimiento del interesado;
- cuando sea una obligación legal;
- a las administraciones públicas para el ejercicio de sus competencias;
- cuando sea necesarios para la ejecución de un contrato;
- y para la protección de intereses vitales del interesado.

La Protección de los Datos



Los responsables deben aplicar las medidas de seguridad y comunicarlas a los empleados que tengan acceso

Los responsables tienen la obligación de aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento de los datos.

Las medidas de seguridad deben garantizar la confidencialidad, integridad, disponibilidad y posibilidad de recuperación de los sistemas y servicios de tratamiento en caso de incidentes.

El responsable del tratamiento deberá obligatoriamente poner en conocimiento de sus empleados, usuarios y colaboradores, las medidas necesarias para que conozcan las normas de seguridad y procedimientos que afecten al desarrollo de sus funciones.

3.- La Seguridad de los Datos Personales.

Las obligaciones comunes que afectan al personal (I)



Confidencialidad	<p>Todo el personal está obligado al secreto profesional, inclusive finalizada la relación laboral. La confidencialidad es extensible a los datos personales, documentación, procedimientos técnicos, especificaciones, parámetros, procesos, programas, datos o información técnica, comercial o financiera que tenga este carácter.</p>
Acceso a datos personales	<p>Solamente se podrá acceder a los datos de carácter personal a los que se esté autorizado y, exclusivamente para el desarrollo de sus funciones laborales, quedando expresamente prohibido su uso para fines privados.</p>
Medidas de seguridad	<p>Todo usuario está obligado a adoptar las medidas de seguridad que la empresa le indique.</p>

3.- La Seguridad de los Datos Personales.

© Lant Advisors, S.L.P.

Las obligaciones comunes que afectan al personal (II)



Cesión de datos	Está absolutamente prohibida la comunicación de datos personales a terceros no autorizados, externos o internos a la entidad, excepto en los casos legalmente previstos, y en aquellos supuestos que sea necesario para el desarrollo de la actividad laboral.
Uso de Periféricos	En el uso de impresoras, fotocopiadoras, escáner y fax, se deberá tener la precaución de que en la bandeja de salida no quede ningún documento que contenga datos personales. La documentación de las bandejas de salida que no le pertenezca, es confidencial.
Puestos de trabajo	Los usuarios son responsables de su puesto de trabajo y, deberán garantizar, en la medida de lo posible, que ninguna otra persona no autorizada pueda ver la información sobre datos personales que muestran sus equipos informáticos o documentación en soporte papel.

3.- La Seguridad de los Datos Personales.

© Lant Advisors, S.L.P.

Las obligaciones comunes que afectan al personal (III)

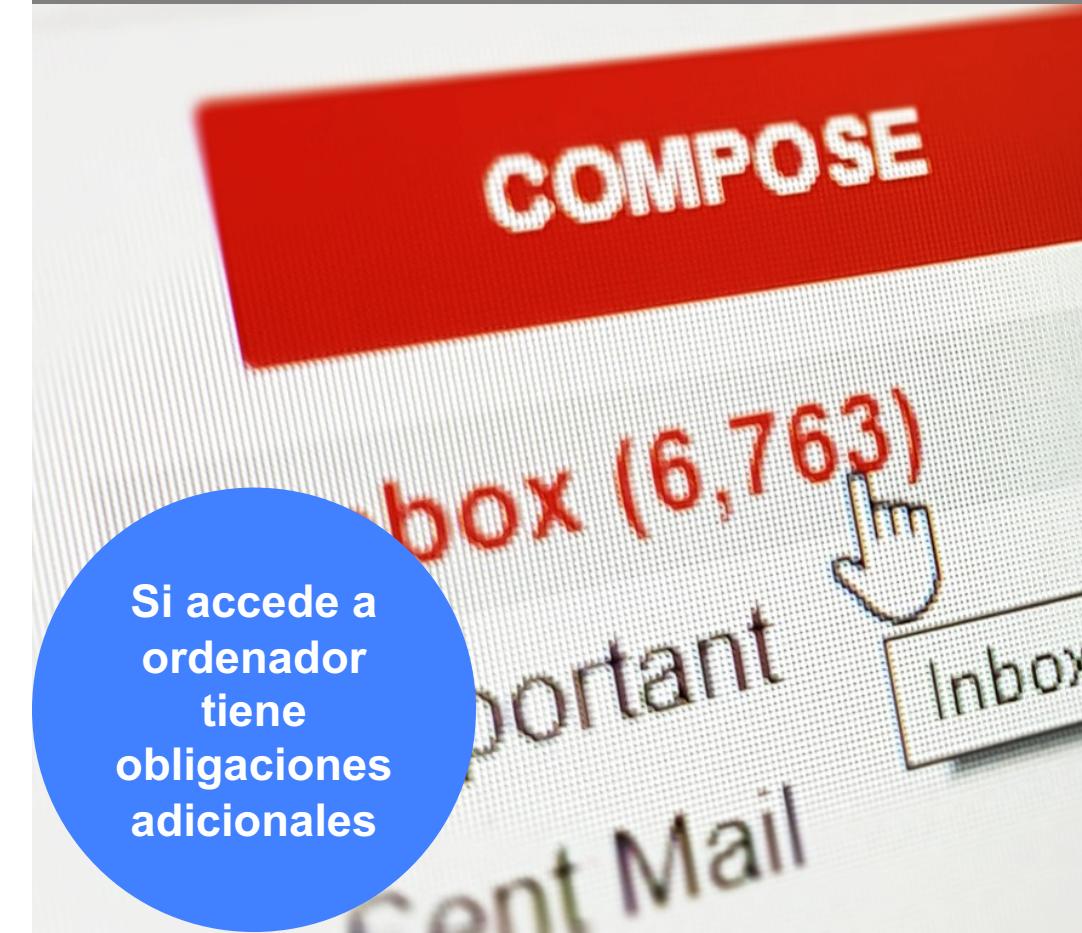


Derechos de los ciudadanos	Todo el personal está obligado a atender los derechos solicitados por terceros (Acceso, rectificación, cancelación, oposición, limitación y portabilidad) y, a ponerlo en conocimiento de su responsable inmediatamente.
Incidencias de seguridad	Cualquier incidencia que afecte a la seguridad de los datos deberá ser comunicada a su responsable. Su conocimiento y no comunicación puede ser considerada como una falta contra la seguridad de los datos personales por parte del usuario.
Dudas Seguridad	Cualquier duda con relación a la confidencialidad y seguridad en el tratamiento de datos personales se debe poner en conocimiento de sus responsables.

3.- La Seguridad de los Datos Personales.

© Lant Advisors, S.L.P.

Las Obligaciones del Personal



Las obligaciones del personal con acceso a informático se refieren a las contraseñas y su confidencialidad, el uso sistemas informáticos, el almacenamiento de Información, el uso de soportes informáticos y de dispositivos portátiles, los accesos remotos o teletrabajo y el almacenamiento de datos en la nube.

Las obligaciones del personal respecto al tratamiento en papel se refieren a la custodia y archivo y a la destrucción, reutilización y salida de documentación.

3.- La Seguridad de los Datos Personales.

Los empleados que accedan a sistemas de información deben utilizarlos de forma adecuada para garantizar la seguridad y confidencialidad de la información y respetando las normas de las que destacamos los siguientes puntos:

- El uso para fines personales debe ser autorizado expresamente por los responsables de la organización.
- La utilización del correo electrónico es estrictamente profesional.
- No se deben almacenar o guardar correos electrónicos privados o de contenido personal en los gestores de correo de la entidad.
- Está prohibido el envío masivo de mensajes de correo electrónico, el abuso en la utilización particular, las cadenas de mensajes, abrir mensajes de correo electrónico donde el remitente no esté plenamente identificado, intentar leer, borrar, copiar o modificar los mensajes de correo electrónico de otros usuarios, etc.
- Se debe utilizar la copia oculta para el envío de correos electrónicos simultáneos a varios destinatarios.
- El acceso y utilización de Internet está limitado a fines profesionales directamente relacionados con las funciones desarrolladas por el trabajador

3.- La Seguridad de los Datos Personales.