PROTECCIÓN DE DATOS DE CARATER PERSONAL

¿Qué son los datos de carácter personal?

- Los datos de carácter personal son **cualquier información concerniente a personas físicas**. Esta información puede ser numérica, alfabética, gráfica o incluso acústica.
- Si queremos saber si una información es personal o no, podemos comprobar si esa información, por sí misma o combinada, puede permitir conocer datos de una persona concreta.
- La información personal es, por lo tanto, cualquier información, por intrascendente que pueda parecer, referente a una persona física, de la cual se pueda conocer quién es su titular.

Algunos ejemplos de datos personales pueden ser:

- Edad
- Domicilio
- Número telefónico
- Trayectoria académica, laboral o profesional
- Patrimonio
- Correo electrónico personal
- Número de seguridad social
- Estado de salud
- Origen étnico y racial
- Características físicas (ADN, huella digital)
- Ideología y opiniones políticas
- Creencias o convicciones religiosas o filosóficas
- Preferencias sexuales, entre otros.
- Estos datos pueden estar contenidos en cualquier soporte como en papel, en la memoria de un equipo informático, o en un DVD.

- Los datos relativos a una persona jurídica (individuo con derechos y obligaciones que existe, pero no como persona física, sino como institución que es creada por una o más personas físicas para cumplir un objetivo social que puede ser con o sin fines de lucro) como puede ser un domicilio, denominación social, CIF, etc. no tienen la consideración de datos de carácter personal, por lo tanto, no le será de aplicación el Reglamento de Protección de Datos.

RGPD

- RGPD es la abreviatura del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

- La UE acordó la reforma de su política de protección de datos, instrumentalizada en la aprobación de un nuevo paquete legislativo entre cuyas medidas se incluye la aprobación del Reglamento RGPD.

- Introduce novedades y mejoras significativas en la protección de este derecho fundamental de la UE.

- El RGPD sustituye todas las normas nacionales anteriores, así como cualquier norma sectorial que contenga regulaciones sobre la protección de datos personales.

¿quién tiene que cumplirlo?

Todas las empresas que manejemos datos de carácter personal, tanto en soporte informático como en papel.(esto es así desde el 2007, aunque la empresa solo tenga datos en fichero papel, también tiene la obligación de cumplir con la normativa)

• Actual Ley de Protección de datos (LOPD-GDD 3/2018)

- La nueva **LOPDGDD o Ley Orgánica de Protección de datos y Garantía de los Derechos Digitales** establece una nuevo marco jurídico para la protección de datos en España, amparada por la normativa europea.
- Se amplía la información que se les debe dar a los usuarios en relación con el tratamiento de sus datos, así como sus derechos en esta materia.
- Se incorpora el concepto de privacidad desde el diseño. Esto se traduce en que la elaboración de los procedimientos empresariales se tiene que realizar teniendo en cuenta la LOPDGDD desde un primer momento.

- # Actual Ley de Protección de datos (LOPD-GDD 3/2018)

- Las brechas en la seguridad que puedan afectar a los datos personales deben ser notificadas en un plazo máximo de 72 horas a la Autoridad de Control correspondiente (Agencia Española de Protección de Datos).

- Si, además, en esa violación se pueden ver afectados datos de carácter sensible y con gran repercusión a los afectados, también se le deberá notificar a los mismos.

• Actual Ley de Protección de datos (LOPD-GDD 3/2018)

- El **consentimiento**, con carácter general, debe ser libre, informado, específico e inequívoco. Las empresas deben revisar la forma en la que obtienen y guardan el consentimiento. Para poder considerar que el consentimiento es “incuestionable”, el Reglamento General de Protección de Datos requiere que haya una declaración de los interesados o una acción positiva que apunte al acuerdo del interesado. La aceptación no puede deducirse del silencio o de la inacción de los ciudadanos.

- Define la figura del Delegado de Protección de Datos.

Derechos de las personas sobre sus datos

¿Qué se entiende por tratamiento de datos?

- En la práctica, cualquier actividad en la que estén presentes datos de carácter personal constituirá un tratamiento de datos, ya se realice de manera manual o automatizada, total o parcialmente, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción

Recabar datos

Registro de actividad del tratamiento

- tendrás que llevar un **Registro de actividad del tratamiento** si empleas a más de 250 personas o realizas tratamientos de datos personales de forma no ocasional o que pueda entrañar riesgos para su privacidad o con categorías especiales de datos.

¿Quién es el responsable del tratamiento de datos?

- El responsable del tratamiento es la persona física o jurídica, pública o privada, que se beneficia, necesita o decide sobre la finalidad, contenido y uso del mismo, directamente o porque así le viene impuesto por una norma legal.

¿Quién es el encargado del tratamiento de datos?

- El encargado del tratamiento es la persona física o jurídica, autoridad, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- En determinados casos, los centros educativos para cumplir sus funciones necesitan contar con la colaboración de otras personas o entidades que no forman parte de su organización, por ejemplo, para el servicio de comedor, servicio médico, transporte o para la realización de actividades extraescolares.
- Estas personas y entidades para prestar sus servicios también tratan los datos de carácter personal de los alumnos y de sus padres o tutores, pero lo hacen por encargo del responsable del tratamiento, es decir del centro o de la Administración educativa.
- Las empresas que realizan este tipo de servicios tienen, en relación con el tratamiento de datos personales que realizan, la consideración de encargados de tratamiento. Es necesario que el tratamiento de datos que implica la prestación del servicio se rija por un contrato que deberá incluir las garantías adecuadas:

DPO

- El *Delegado de Protección de Datos* o **DPO** tiene la responsabilidad de que se cumplan las leyes relacionadas a, como dice su cargo, la protección de los datos de la compañía. Es un cargo que puede formar parte de la planta de la empresa, pero también puede ser externo, y ya que lo más importante tiene que ver con sus conocimientos especializados al respecto.
- El **DPO** se transforma en un garante de la compañía sobre la protección de datos, y de cumplir con las normas respectivas, y por lo mismo se destaca la relevancia de sus conocimientos en derecho.

Funciones del DPO

- la principal función del **DPO** tiene relación con el cumplimiento de la protección de los datos de la empresa. De todas formas, no es la única, por lo que revisaremos en detalle las más importantes.
- Apoyar en el tratamiento de los datos al personal encargado. Considerando el conocimiento del DPO al respecto, se preocupa de que las obligaciones de la ley se cumplan, junto a cualquier otra disposición.
- En línea con el punto anterior, el **DPO** debe supervisar que se cumplan con el RGPD y todas sus normativas. En ese sentido, la asignación de responsabilidades, preparación de los colaboradores y generar un cambio de conciencia también es parte de sus funciones.
- Asesorar a la compañía con respecto a la evaluación del impacto que puede tener la protección de datos y su buen cumplimiento.
- Cooperar con todo el control relacionado y ser el contacto para la autoridad de control en cuanto al tratamiento de sus responsabilidades.

¿Cuándo debería una empresa tener un Delegado de Protección de Datos?

- Autoridad u organismo público, a excepción de los tribunales de justicia.
- Observación habitual y sistemática de interesados, como puede ser la banca, aseguradora o medios de comunicación, entre otros.
- Categorías especiales de datos, como puede ser por información de origen étnico, política, religioso u otros. Por ejemplo, un partido político, una iglesia o un hospital.
- Hay datos relacionados a temas penales, como puede ser un gabinete jurídico.

DPO (Delegado Protección Datos)

- El **DPO** ha de tener total acceso a la cúpula directiva para asesorar y reformar aquellos procesos o métodos que sean necesarios para el cumplimiento de las nuevas políticas proactivas en esta materia.
- El RGPD establece una serie de entidades en las que será obligatoria la presencia de un DPD, por ejemplo a las federaciones deportivas o los clubes deportivos por tener entre sus actividades principales el tratamiento a gran escala de datos sensibles o la observación habitual y sistemática de un número elevado de interesados.

¿Qué se entiende por cesión de datos?

- La cesión de datos supone su revelación a una persona distinta de su titular. Los destinatarios o cesionarios de los datos serán las personas físicas o jurídicas, autoridades públicas, servicios u otros organismos a los que se les comuniquen.

¿Cuándo se produce una transferencia internacional de datos?

- Siempre que los datos personales se envían fuera del ámbito de Espacio Económico Europeo (EEE), que comprende todos los Estados miembros de la Unión Europea, más Noruega, Islandia y Liechtenstein, se produce una transferencia internacional de datos, ya se realice para que el destinatario de los datos preste un servicio al centro educativo o para que los trate para una finalidad propia.

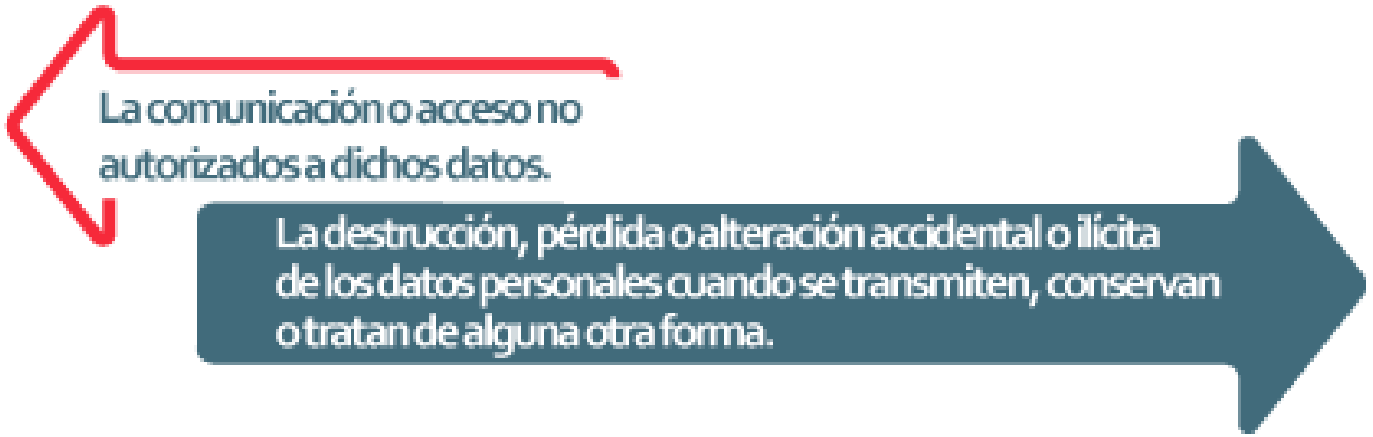
¿Cómo cumplo?

- Adecuar tus procedimientos y canales para informar, recabar el consentimiento, permitir el ejercicio de los derechos y notificar en caso de brecha de seguridad que afecte a la privacidad.
- Revisar los contratos con los encargados del tratamiento si los tuvieras.
- Poner en marcha políticas para garantizar la seguridad de los tratamientos.
- Concienciación

¿Qué pasa si no cumplo?

- Cualquier ciudadano de la UE tiene derecho a **presentar reclamaciones de forma individual o colectiva** si considera que el tratamiento de sus datos personales vulnera el RGPD. También, al ser la privacidad un derecho fundamental, tendrá derecho a la **tutela judicial efectiva** y a la **indemnización** por los **daños y perjuicios** sufridos a consecuencia de una infracción del RGPD.
- Las *autoridades* podrán investigar y corregir las infracciones. Para ello estarán en disposición de ordenar al responsable o al encargado **que facilite información, lleve a cabo auditorías u obtenga acceso a los datos, locales y equipos.**
- Las sanciones por infracción podrán ir, desde advertencias si la infracción es posible, apercibimientos y limitaciones temporales, hasta prohibir el tratamiento, ordenar supresión de datos e imponer multas.

Si tengo problemas: Informar brechas seguridad



- **¿Cómo me ayuda la tecnología a garantizar la seguridad de los tratamientos?**

Medidas Seguridad

Determinar dónde están ubicados los datos, clasificarlos según su criticidad, monitorizar su uso, conocer quién accede, cuando se borran y cifrarlos cuando sea necesario. Se pueden utilizar distintas soluciones de **prevención de fuga de información.**

Evitar accesos no autorizados y restringir el acceso a los datos aplicando principios de mínimos privilegios mediante sistemas de **gestión de identidad y Autenticación**.

Tener controlados todos los **dispositivos** y **soportes** con herramientas que nos permitan hacer **inventarios** de los mismos y del **software** instalado verificando a su vez que sea **legítimo** y esté **actualizado**.

Cifrar los datos, para lo cual se utilizarán **herramientas de cifrado**.

Recuerda: el cifrado garantiza la confidencialidad y la integridad, **reduce el riesgo de sanciones** y evita que tengamos que informar a los usuarios en caso de brecha de seguridad.

Realizar *backups* mediante instrumentos específicos de **contingencia y continuidad**.

Instalar y activar herramientas **anti-fraude y anti-malware.**

Proteger las comunicaciones tanto por cable como inalámbricas con equipos específicos, y en particular con **cortafuegos**, para evitar que puedan estar accesibles a terceros no autorizados. Igualmente tendremos que asegurar las comunicaciones con redes privadas virtuales o **VPN** u otros mecanismos que las cifren y permitan autenticar a los extremos.

Recomendaciones

- Análisis de riesgos o auditoría del estado informático de la entidad.
- Copias de seguridad a más de 1 km. de distancia del origen de los datos.
- Herramientas de resistencia o fortificación del sistema, redes y equipos.
- Alarma informática para detectar intrusiones o brechas de seguridad, y así poder comunicarlas en menos de 72 horas a la Agencia Española de Protección de Datos.
- Defensa perimetral y de dispositivos (Internet de las cosas) a través de firewall de nueva generación.
- Antivirus de nueva generación adecuadamente integrados en los equipos informáticos.

Pasos Elaborar documento

- **Paso 1: Conocer los datos personales que recopila y usa en su empresa y los motivos por los que los necesita**
- **Paso 2: Informar a sus clientes, empleados y otras personas cuando necesite recopilar sus datos personales**
- **Paso 3: Conservar los datos personales solo durante el tiempo necesario**
- **Paso 4: Proteger los datos personales que está procesando**
- **Paso 5: Mantener documentación sobre sus actividades de procesamiento de datos**
- **Paso 6: Asegurarse de que los subcontratistas respeten las reglas**
- **Paso 7: Asignar a alguien para supervisar la protección de datos personales**

Paso1

•Identificar todas las **fuentes** de datos personales de nuestros tratamientos, catalogar todos los **agentes** responsables y los tipos de **operaciones** que se hacen con esos datos durante todo su ciclo de vida: captura, clasificación y almacenamiento, uso, cesión o transferencia y destrucción.
•Ser **exhaustivos** con los datos que se recogen: ¿dónde se almacenan?, ¿durante cuánto tiempo?, ¿en un fichero o en una base de datos?, ¿en qué equipos? ¿siguen los *principios del tratamiento del RGPD* ?
•Hacer un **diagrama de flujo de datos del tratamiento**, es decir desde que se recogen hasta que se utilizan o desechan con las transformaciones intermedias.
•Priorizar, es decir, analizar en primer lugar a los agentes involucrados en el tratamiento y las acciones problemáticas sobre los datos, es decir, aquellas que pueden tener un **efecto adverso sobre la privacidad** de las personas.

Paso 2 : Informar a sus clientes, empleados y otras personas cuando necesite recopilar sus datos personales

- Plantillas de comunicación

Paso5: Documentación Actividades

Información	Ejemplos
El propósito del procesamiento de datos	Alertar a los clientes sobre ofertas especiales, como proporcionar entrega en casa; proveedores de pago; cobertura de salario y seguridad social para empleados
Los tipos de datos personales	Detalles de contacto de los clientes; detalles de contacto de los proveedores; datos de empleados
Las categorías de personas interesadas	Empleados; clientes; proveedores
Las categorías de destinatarios	Autoridades laborales; autoridades fiscales
Los períodos de almacenamiento	Los datos personales de los empleados hasta la finalización del contrato laboral (y las obligaciones legales relacionadas); los datos personales de los clientes hasta la finalización de la relación contractual/cliente
Las medidas de seguridad técnicas y organizativas para proteger los datos personales	Soluciones del sistema de TI actualizadas periódicamente; ubicación protegida; control de acceso; cifrado de datos; copia de seguridad de datos
Si los datos personales se transfieren a destinatarios fuera de la UE	Uso de un procesador fuera de la UE (por ejemplo, almacenamiento en la nube); ubicación de datos del procesador; compromisos contractuales

Paso 6: Asegurarse de que los subcontratistas respeten las reglas

- Elaborar contratos y asegurar proveedores los cumplen