RGPD

O COMO SU IMPLEMENTACIÓN NOS SALVÓ LA BILLETERA

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

INDICE

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

- Introducción al RGPD
- Marco Normativo y Consecuencias derivadas su incumplimiento.
- Tipos de Datos y como Clasificarlos
- Roles
- Implementación de las Medidas
- Necesidad de Realizar Auditorías Periódicas

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

WHOAMI

- **Nombre**: Diego Martinez
- **Puesto:** Responsable Dpto de Ciberseguridad Cyberhelp
- **Contacto:**dmartinez@helphone.com

Experiencia Profesional

- 8 años de Analista Forense Freelance en varias audiencias provinciales
- 2 años Consultor de SDLC Consultora Ciberseguridad
- 2 años Analista y Co-Fundador del Laboratorio de Análisis de Software de Entidad Bancaria
- 1 año Miembro de Equipo de Ciberseguridad de Entidad Bancaria (Red Team)
- 4 años Miembro del equipo de Respuesta ante Incidentes de Entidad Bancaria (DFIR Team)
- Responsable de Departamento Ciberseguridad Cyberhelp

¿De qué vamos a hablar hoy…?

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Fuente Xataka

España, el país que más multas pone

Desde que empezara a ser de obligado cumplimiento hace ahora casi tres años, ha habido más de 281.000 notificaciones de incumplimiento. **Los países que más denuncias acumulan son Alemania (77.747), Países Bajos (66.527) y Reino Unido** (30.536). En el extremo opuesto se encuentran Francia e Italia, que registraron 5.389 y 3.460 infracciones, respectivamente.

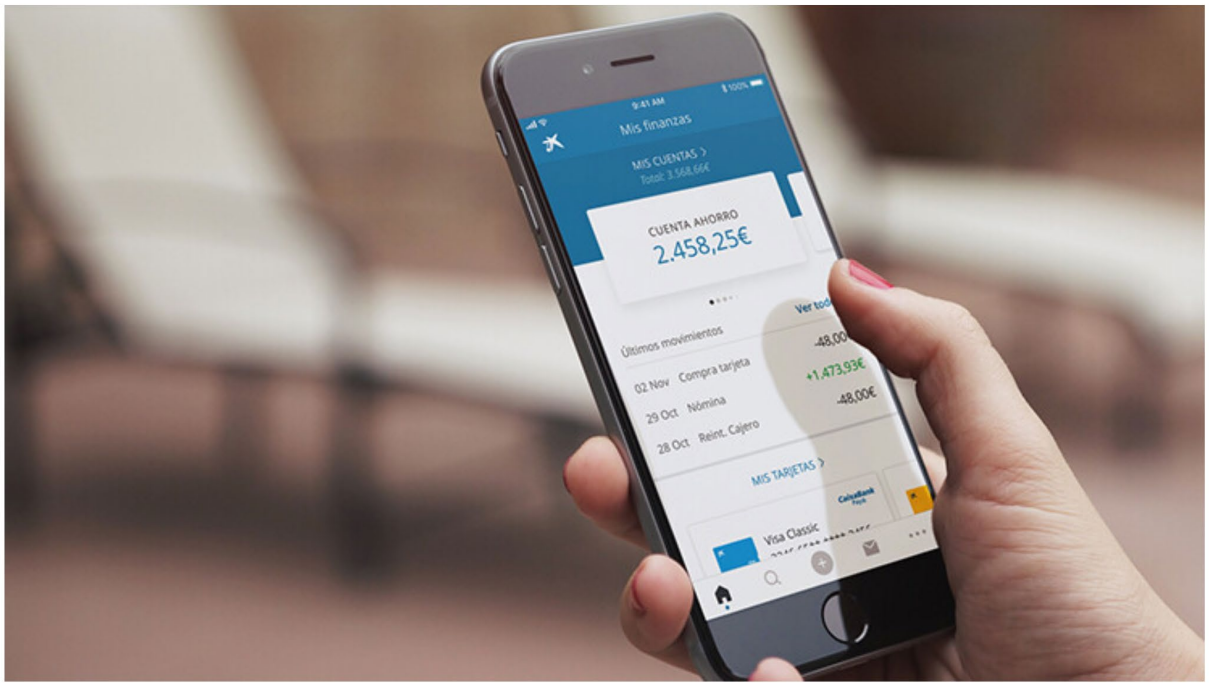
Según los datos de Enforcement Tracker, España es el quinto país que más importe en penalizaciones ha puesto: 15,5 millones repartidas en 173 penalizaciones. Este número nos convierte, según este portal, en el **país que más multas acaba poniendo** por infracciones de GDPR. La última que ha puesto la Agencia de Protección de Datos en España supone, además, un nuevo récord en nuestro país: 6 millones de euros.

¿De qué vamos a hablar hoy…?

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Multa récord de la Agencia de Protección de Datos a Caixabank: 6 millones de euros por forzar la cesión de datos personales



14 Enero 2021 - Actualizado 14 Enero 2021, 12:27

21 Comentarios

¿De qué vamos a hablar hoy…?

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

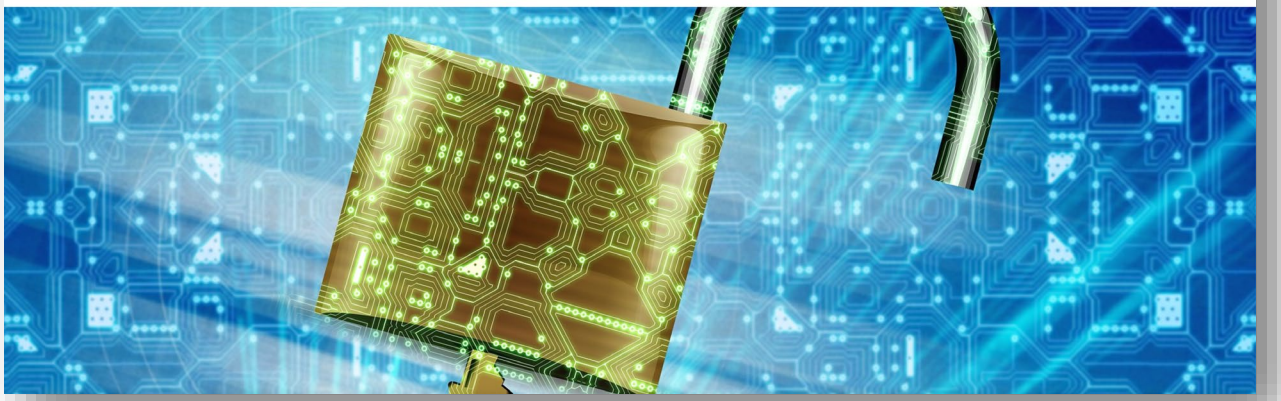
Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,
la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a la entidad CAIXABANK, S.A., con NIF ***A08663619***, por una infracción de los artículos 13 y 14 del RGPD, tipificada en el artículo 83.5.b) y calificada como leve a efectos de prescripción en el artículo 74.a) de la LOPDGDD, una multa por importe de 2.000.000 euros (dos millones de euros).

SEGUNDO: IMPONER a la entidad CAIXABANK, S.A., por una infracción del artículo 6 del RGPD, tipificada en el artículo 83.5.a) y calificada como muy grave a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD, una multa por importe de 4.000.000 euros (cuatro millones de euros).

NOTICIAS JURÍDICAS

Protección de datos: España lidera el ranking de multas impuestas por incumplir el RGPD en 2020



¿De qué vamos a hablar hoy…?

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Multa de 5 millones de euros de la Agencia Española de Protección de Datos (AEPD) a BBVA por varias infracciones del RGPD

14/12/2020 GONZALO SÁNCHEZ-JARA NO HAY COMENTARIOS

Multa en Italia de 12,25 millones de euros a Vodafone por numerosas infracciones del RGPD relacionadas con su actividad de telemarketing

30/11/2020 GONZALO SÁNCHEZ-JARA NO HAY COMENTARIOS

El pasado 12 de noviembre, la Agencia de Protección de Datos Italiana (el "**Garante per la protezione dei dati personali**" o el "**Garante**") impuso a la empresa de telecomunicaciones Vodafone Italia S.p.A. ("**Vodafone**") una multa de 12,25 millones de euros por numerosas infracciones del RGPD.

Fuente: rgpdblog.com

¿Nos hacemos un top ten?

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Multa n.º 1: 250.000 euros
Reclamado: Liga Nacional de Fútbol Profesional
Procedimiento Sancionador: PS/00326/2018
Infracción: Artículo 5.1.a) del RGPD
Fecha de publicación: 20 de agosto de 2019

Motivo de la reclamación:
La creación por el reclamado de una aplicación móvil que podía captar de forma indiscriminada sonido ambiente del lugar donde se encontrara el usuario. Esto podía implicar la captación de conversaciones con terceros que podrían desvelar datos personales.

Multa n.º 2: 120.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00144/2019
Infracción: Artículo 6.1 del RGPD
Fecha de publicación: 19 de septiembre de 2019

Motivo de la reclamación:
El reclamado tenía contratado a nombre del reclamante varios servicios los cuales este no había contratado.

Multa n.º 3: 120.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00235/2019
***Infracción: Artículos 6.1.a) y 5.1.a) del* RGPD**
Fecha de publicación: 27 de febrero de 2020

Motivo de la reclamación:

La recepción del hijo menor de edad del reclamante de una carta del reclamado en la que le comunicaba que había contraído con ellos una deuda de 93,77 euros y que en el caso de impago se procedería a su inclusión en una lista de morosos.

¿Nos hacemos un top ten?

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Multa n.º 4: 100.000 euros
Reclamado: Endesa Energía XXI, S.L.U.
Procedimiento Sancionador: PS/00074/2019
Infracción: Artículo 5.1.f) del RGPD
Fecha de publicación: 22 de mayo de 2019

Motivo de la reclamación:
Un tercero contactó con el reclamado para efectuar un cambio en el contrato de suministro eléctrico en el que la reclamante figuraba como apoderada

Multa n.º 5: 100.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00405/2019
Infracción: Artículo 6.1 del RGPD
Fecha de publicación: 3 de febrero 2020

Motivo de la reclamación:
El reclamante recibió un e-mail del reclamado informándole de la facturación de una línea que el reclamante manifiesta no haber contratado.

Multa n.º 6: 100.000 euros
Reclamado: Vodafone España, S.A.U.
Procedimiento Sancionador: PS/00186/2020
Infracción: Artículo 6.1 del RGPD
Fecha de publicación: 1 de septiembre de 2020

Motivo de la reclamación:
El reclamante ha vuelto a recibir en su dirección de correo electrónico un aviso de disponibilidad de factura electrónica procedente del reclamado, lo cual constituye una reincidencia de los hechos sancionados por la AEPD en el procedimiento sancionador PS/00278/2019.

Y podríamos seguir mas y mas y mas…

Conclusiones:

A la vista de los datos, podemos concluir que:

- ***Siete de las infracciones del ranking son consecuencia de la falta de licitud del tratamiento de datos personales (Art. 6.1 del RGPD).***
- ***Dos de las infracciones del ranking surgen por el incumplimiento del Principio de Confidencialidad (Art. 5.1.f) del RGPD).***
- ***Dos de las infracciones son por el incumplimiento del Principio de Licitud, Lealtad y Transparencia (Art. 5.1.a) del RGPD).***
- ***Vodafone España S.A.U. acapara el 50% de las multas del ranking.***
- ***Las empresas del sector de telecomunicaciones representan el 60% de las multas del ranking.***
- ***La mitad de las multas del ranking fueron impuestas en el 2019 y la otra mitad en el 2020.***
- ***Las multas impuestas por la AEPD son más moderadas en cuantía en relación con otras multas que hemos visto en Europa (ej. Google, TIM SpA, o Post AG).***
- ***Las diez multas del ranking suman un total de 1.095.000 euros.***

¿Que es el RGPD?

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Reglamento General de Protección de Datos

General Data Protection Regulation

Norma 2016/679 adoptada por el Parlamento Europeo el 27 de abril de 2016 en relación con la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Sustituye a la "Directiva de 1995" sobre protección de datos Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995

https://www.boe.es/doue/2016/119/L00001-00088.pdf

¿Por qué el RGPD?

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales

La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa.

Una solida protección de datos y de alto nivel es una condición esencial para <u>GANAR CONFIANZA</u> y a su vez es "<u>CLAVE PARA EL DESARROLLO ECONÓMICO</u>" que por otra parte requiere de una <u>libre circulación de los datos personales dentro de la unión</u>

¿Por qué el RGPD?

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

*La protección de datos tiene como objetivo salvaguardar un **EQUILIBRIO JUSTO Y RAZONABLE** entre los intereses de los individuos y los de la comunidad en relación con el tratamiento de datos personales.*

Principios Reguladores del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

- *La recopilación y posterior uso y divulgación de datos personales deben estar **sujetos a la ley***
- *Las Leyes deben ser **"generales"** que se aplican a todas las entidades públicas y privadas que procesan datos personales*
- *La leyes deben contener ciertas **normas sustantivas básicas** que contengan los **principios básicos** de la protección de los datos personales y los derechos de los ciudadanos.*
- *La aplicación de esas leyes debe ser **supervisada por órganos especiales** de supervisión*

aepd agencia española protección datos

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

Objetivos del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

- ✓ Proteger los datos de carácter personal
- ✓ Contribuir al espacio común de libertad, seguridad, justicia, progreso económico, social dentro de la unión europea
- ✓ Armonizar la protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos y garantizar la libre circulación de estos datos dentro de la Unión Europea
- ✓ Generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior.

¿RGPD en España?

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

LOPDGDD - Ley de Protección de Datos y Garantía de Derechos Digitales

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales adapta el derecho español al modelo establecido en la RGPD

https://www.boe.es/eli/es/lo/2018/12/05/3/con

Autoridades de Control

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

aepd agencia española protección datos

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

apdcat
Autoritat Catalana de Protecció de Dades

Consejo de Transparencia y Protección de Datos de Andalucía

¿Tengo que cumplir la RGPD?

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

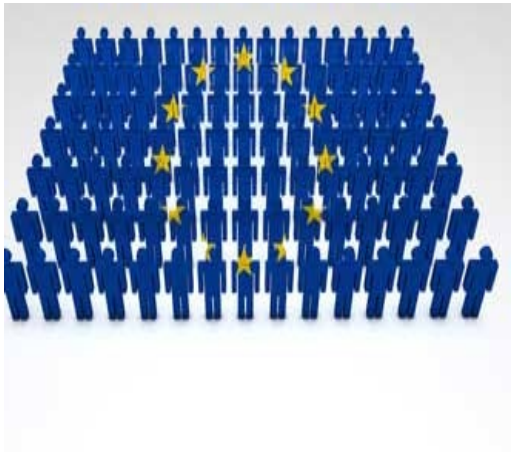
- Empresas
- Sociedades
- Organizaciones
- Asociaciones
- Autónomos

¿Qué pasa si no cumplo?

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

¿Quién puede denunciar?

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.



¿Dónde se denuncia?

Ante la Agencia de Protección de Datos

aepd agencia española protección datos

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

Marco Normativo del Procedimiento

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE
(Reglamento General de Protección de Datos - RGPD)

Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

¿Cuáles son las Sanciones?

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Los artículos 83 y 84 del Reglamento europeo recogen, de manera general, las condiciones para la imposición de multas administrativas y el rango que pueden alcanzar las multas según el RGPD.

Los artículos 70 a 78 de la LODPGDD que detalla el régimen sancionador en materia de protección de datos en España

- Sujetos responsables
- La graduación de las infracciones
- Plazos de prescripción
- Sanciones aplicables

¿Criterio Sancionador?

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

- La naturaleza, gravedad y duración de la infracción, el número de ciudadanos afectados, así como el nivel de los perjuicios ocasionados.
- Si la infracción es causa de una negligencia o hay intencionalidad detrás de ella.
- Si el encargado o el responsable del tratamiento ha tomado medidas para reducir los daños o perjuicios ocasionados a los interesados.
- El grado de responsabilidad del responsable o encargado, teniendo en cuenta también las medidas de seguridad aplicadas.
- Si se han cometido infracciones anteriores.
- Si se ha cooperado y en qué medida con la autoridad de control para solucionar la infracción y los daños causados.
- Las categorías de datos personales afectadas.
- Si la infracción se notificó a la autoridad competente por el encargado o responsable.
- La existencia de medidas técnicas y organizativas previas para evitar la comisión de infracciones por negligencia.
- Otros factores agravantes o atenuantes que se puedan aplicar.

Tipos de infracciones

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Muy Graves Art 72 LOPDGDD	• Uso de los datos para una finalidad diferente a la pactada. • Omisión del deber de correcta información al afectado. • Exigencia de un pago para poder acceder a los datos propios almacenados. • Transferencia internacional de información sin garantías.
Graves Art 73 LOPDGDD	• Datos de un menor recabados sin consentimiento. • Falta de adopción de medidas técnicas y organizativas necesarias para la efectiva protección de datos. • Incumplimiento de nombrar responsable o encargado de tratamiento de datos.
Leves Art 74 LOPDGDD	Las restantes no contempladas en los grupos anteriores. Algunos ejemplos: • No transparencia de la información. • Incumplimiento de no informar al afectado cuando lo haya solicitado. • Incumplimiento por parte del encargado de sus obligaciones.

Cuantías de las Sanciones

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

El RGPD establece las siguientes cuantías para las sanciones:

- 10 millones de euros o el equivalente al 2% del volumen de negocio total anual para las infracciones comprendidas en el apartado 4, letras a, b y c del artículo 83 del RGPD

- 20 millones de euros o el equivalente al 4% del volumen de negocio total anual para las infracciones comprendidas en el apartado 5, letras a, b, c, d y e y apartado 6 del artículo 83 RGPD

Plazo de Prescripción de las Sanciones

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

El plazo de prescripción de las sanciones varía en función del importe de la sanción

(Art 78 de la LOPDGDD)

Las sanciones por un importe superior a 300.000 euros	*3 años*
Las sanciones por importe comprendido entre 40.001 y 300.000 euros	*2 años*
Las sanciones por importe igual o inferior a 40.000 euros	*1 año*

El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla

Apercibimientos

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Medida de carácter excepcional que consiste en la notificación para que el infractor adopte las medidas correctoras que en ella se le indiquen.

La Agencia Española de Protección de Datos decide si impone una sanción económica o un apercibimiento, en función de la naturaleza de los hechos sancionados.

Una vez se recibe un apercibimiento, se tiene que acreditar que se han tomado las medidas solicitadas por la Agencia.

Ejemplos de Sanciones

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

British Airways: Sanción de 204 Millones de Euros

Falta de seguridad en la empresa, cuando esta sufrió una brecha de seguridad que dejó al descubierto la información de las tarjetas de crédito de 500.000 clientes, así como información de vuelos y reservas.

Cadena de hoteles Marriott: Sanción 110 Millones de Euros

No llevar a cabo una ”due diligence” adecuado al adquirir la empresa Starwood, que habría provocado una brecha de seguridad con la que quedaron expuestos unos 339 millones de registros de clientes de 31 nacionalidades del EEE (Espacio Económico Europeo).

Ejemplos de Sanciones

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Google*:* Sanción de 50 millones de euros

Información sobre el tratamiento de datos personales a disposición de los usuarios no era fácil de acceder ni entender.

- Falta de transparencia dado las dificultades que tenían los usuarios de Google para acceder a la información,
- Información insuficiente y deficiente en torno al tratamiento de datos personales
- La falta de una base de legitimación para el tratamiento de anuncios personalizados.

Sanciones AEPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Agencia Española de Protección de Datos (AEPD) ha sido con creces la autoridad de control europea que más ha hecho uso de su potestad sancionadora.
(Datos de Enero a Agosto de 2020)

España lidera el ranking de multas impuestas por incumplir el RGPD en 2020

https://www.economistjurist.es/noticias-juridicas/proteccion-de-datos-espana-lidera-el-ranking-de-multas-impuestas-por-incumplir-el-rgpd-en-2020/

Sanciones AEPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

BBVA: Sanción de 5 millones de Euros

CaixaBank: Sanción de 6 millones de Euros

Hacer uso de los datos personales de sus clientes sin el consentimiento de los mismos.

Tipos de Información

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

¿Qué son los Datos Personales?

Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

Art 4. del RGPD

Tipos de Información

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Los datos personales pueden estar:

- ***en formato digital***

Ficheros de todo tipo (texto, imagen, multimedia, bases de datos,...), pasando por los programas y aplicativos que los utilizan y gestionan, hasta los equipos y sistemas que soportan estos servicios

- ***en otros soportes físicos***

Papel, película fotográfica, etc...

Tipos de Información

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Categorías de datos según la RGPD

- ❑ Datos Especialmente Protegidos o “Datos Sensibles”
- ❑ Datos de Naturaleza Penal
- ❑ Datos NO Sensibles o básicos

Todos aquellos que no sean considerados datos sensibles o "categorías especiales de datos" o bien que no se traten de modo específico (como los datos relativos a infracciones y condenas penales), se considerarán como datos no sensibles o como antiguamente se denominaban de un modo más sencillo "datos básicos"

Tipos de Información

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Se pueden considerar como **Datos NO Sensibles o Básicos** los siguientes:

Datos identificativos
Nombre, dirección, *email*, teléfono, firma, imagen, voz y DNI.

Características personales
Estado civil, fecha/lugar de nacimiento, características físicas, edad, nacionalidad, sexo y lengua materna.

Circunstancias sociales
Aficiones, estilo de vida, propiedades/posesiones y características de la vivienda.

Información académica o profesional
Formación, historial de estudiante, experiencia profesional y pertenencia a asociaciones profesionales

Detalles del empleo
Puesto de trabajo y profesión.

Información comercial
Licencias comerciales, suscripciones a publicaciones o medios de comunicación y creaciones literarias, artísticas o científicas.

Información económico-financiera
Cuenta bancaria, préstamos, seguros, ingresos o rentas, tarjeta de crédito, planes de pensiones, datos económicos de la nómina e impuestos.

Datos de transacciones
Bienes y servicios suministrados por el afectado y transacciones o indemnizaciones.

Tipos de Información

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Los datos especialmente protegidos o sensibles requieren mayor protección.

El nuevo Reglamento Europeo de Protección de Datos recoge como categorías especiales de datos:

- **Origen étnico o racial.**
- **Opiniones políticas, convicciones religiosas o filosóficas.**
- **Tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física.**
- **Afiliación sindical.**
- **Datos relativos a la salud.**
- **Datos relativos a la vida sexual o la orientación sexual de una persona física.**

Tipos de Información

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

El RGPD prohíbe el tratamiento de este datos sensibles o de categoría especial, excepto:

Si hay consentimiento para fines específicos

Cuando el interesado dé su consentimiento explícito para el tratamiento de dichos datos para fines específicos, excepto si está prohibido por una ley vigente.

Si es necesario para alguna finalidad específica

- Para proteger intereses vitales del interesado en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.
- Para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social.
- Por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios.
- Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.

Si son manifiestamente públicos
Cuando el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos.

Tipos de Información

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Datos de naturaleza penal

Los datos personales sobre **denuncias, procedimientos o condenas penales**
NO son datos de Categoría Especial.

Para procesar datos personales sobre condenas o delitos penales, debes tener una base legal y una autoridad legal o autoridad oficial para el procesamiento.

Datos que NO son considerados Datos Personales

- Los **datos anonimizados** siempre y cuando no sea posible reidentificar a la persona física

- Los datos referentes a **personas jurídicas.**

Roles de Usuarios

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

El Interesado

El Responsable del Tratamiento

El Encargado del Tratamiento

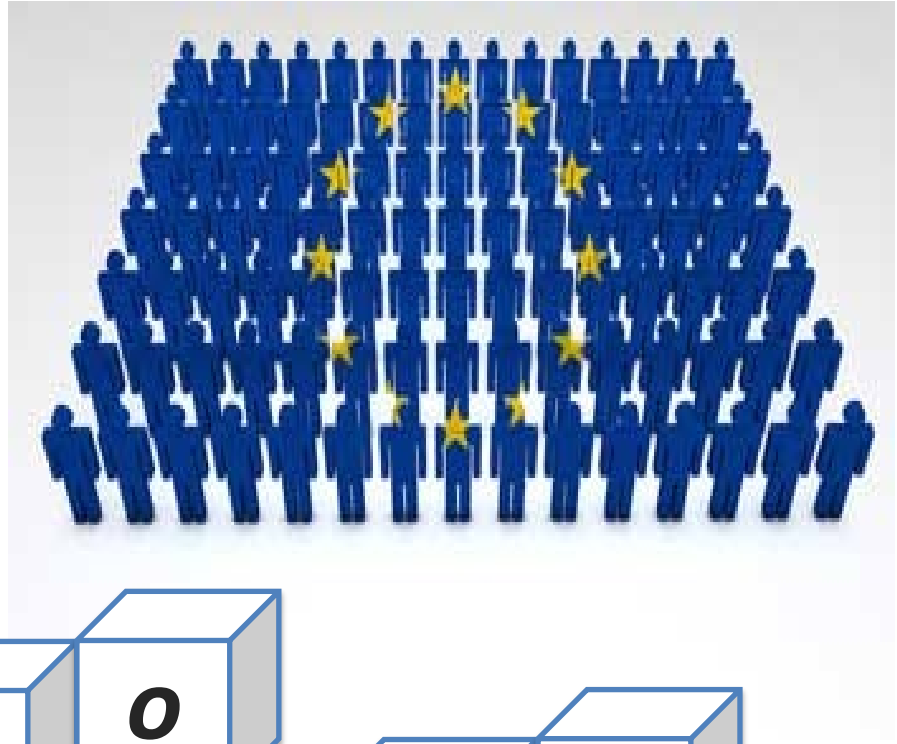
El Delegado de Protección de Datos

Roles de Usuarios

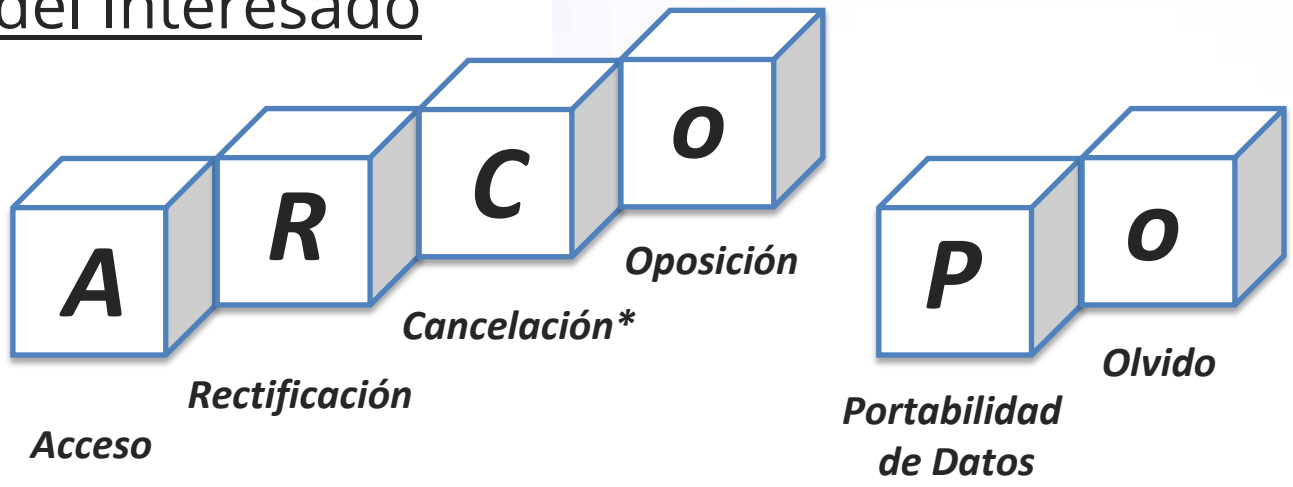
HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

El Interesado.

Serían los individuos que se encuentren en la Unión Europa cuyos datos son tratados.



Derechos del Interesado



Roles de Usuarios

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Responsable del Tratamiento

Art 4 punto 7 de la RGPD

«responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

Roles de Usuarios

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Responsable del Tratamiento

Obligaciones de los responsables (Art 24 de la RGPD)

- Implementación de medidas técnicas y organizativas apropiadas para garantizar el procesamiento legal de datos personales
- Implementar políticas adecuadas de protección de datos
- Llevar a cabo una evaluación de impacto de privacidad cuando sea necesario
- Adherirse a los códigos de conducta elaborados por las autoridades de supervisión en los Estados miembros
- Considere la protección de datos por diseño y por defecto en las actividades de procesamiento
- Demostrar el cumplimiento del Reglamento. Los controladores pueden designar solo aquellos procesadores que garanticen el cumplimiento de los requisitos del GDPR.

Roles de Usuarios

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Encargado del Tratamiento

Art 4 punto 8 de la RGPD

«encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

Roles de Usuarios

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Encargado del Tratamiento

Art 28 de la RGPD

"Donde se lleve a cabo tratamiento debe ser realizado en nombre de un responsable, el cual debe usar solo encargados que ofrezcan suficientes garantías para implementar las medidas técnicas y organizacionales apropiadas de manera tal que el tratamiento cumpla los requerimientos de esta regulación y asegure la protección de los derechos del interesado."

Roles de Usuarios

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Encargado del Tratamiento

Art 28 de la RGPD

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

Roles de Usuarios

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Ejemplo: RESPONSABLE vs ENCARGADO

Una Cervecería que tiene muchos empleados firma un contrato con una empresa de nóminas, para poder pagarles los salarios.

La cervecería indica a la empresa de nóminas cuándo deben pagarse las nóminas, cuándo un empleado abandona la empresa o si tiene un aumento de sueldo, y proporciona toda la demás información sobre la nómina y el pago.

La Empresa de Nóminas proporciona el sistema informático y conserva los datos de los empleados.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_es

Roles de Usuarios

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Delegado de Protección de Datos (DPD o DPO)

Son personas físicas o jurídicas en las que recae la **responsabilidad de la protección de datos de las empresas.** Esta figura puede ser interna o externa a la empresa y no es obligatoria en todos los supuestos.

Es un **garante del cumplimiento de la normativa** en las organizaciones y asesora a la dirección de la empresa y el personal sobre las correctas medidas a tomar.

Figura Obligatoria para:

- ❑ las empresas públicas
- ❑ las que tengan un tratamiento a gran escala o las que recojan datos especialmente sensibles o relativos a condenas o infracciones penales.

Roles de Usuarios

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

LOPDGDD - Artículo 34. Designación obligatoria de un DPD

- Colegios profesionales y sus consejos generales.
- Centros docentes que ofrezcan enseñanzas de los niveles establecidos en la legislación, así como Universidades públicas y privadas.
- Entidades que exploten redes y presten servicios de comunicaciones electrónicas, cuando traten de forma sistemática datos personales a gran escala.
- Prestadores de servicios de la sociedad de la información cuando elaboren perfiles a gran escala.
- Entidades de ordenación, supervisión y solvencia de entidades de crédito.
- Establecimientos financieros de crédito.
- Entidades aseguradoras y reaseguradoras.
- Empresas de servicios de inversión.
- Distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.
- Entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito.
- Entidades que desarrollen actividades de publicidad y prospección comercial cuando lleven a cabo tratamientos basados en preferencias de los titulares o realicen elaboración de perfiles.
- Centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Exceptuando profesionales que ejerzan su actividad a título individual.
- Entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.
- Operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos.
- Empresas de seguridad privada.
- Federaciones deportivas que traten datos de menores de edad.

Roles de Usuarios

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Sanciones relacionadas con el DPD

La AEPD multó con 25.000 y 50.000 euros, respectivamente, a Glovo y a Conseguridad por no contar con la figura del delegado de protección de datos ya que hacían un tratamiento de datos a gran escala (Infracción Grave)

Roles de Usuarios

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Delegado de Protección de Datos (DPD o DPO)

Artículo 39 del RGPD

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

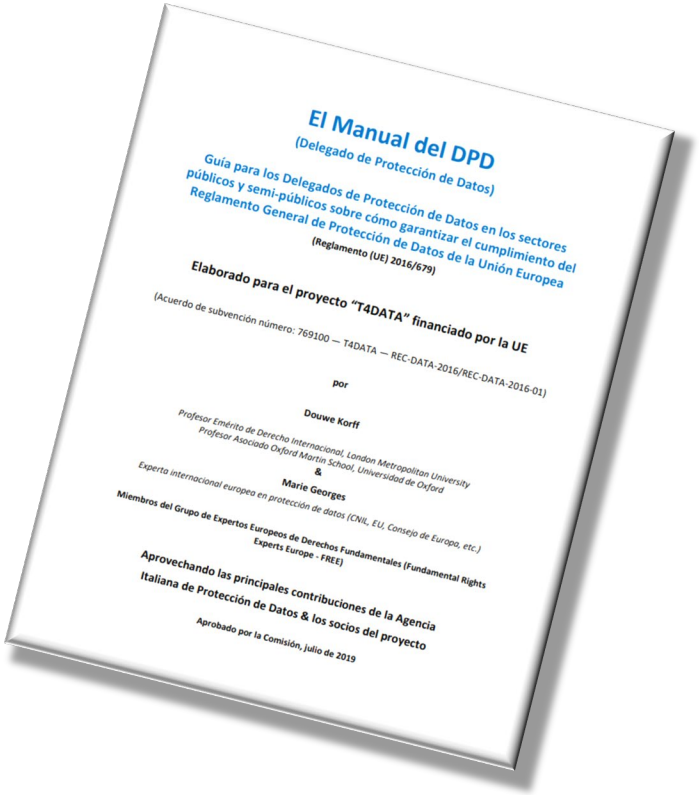
Roles de Usuarios

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Delegado de Protección de Datos (DPD o DPO)

El Manual del DPD (Delegado de Protección de Datos) de la AEPD


El Manual del DPD
(Delegado de Protección de Datos)
Guía para los Delegados de Protección de Datos en los sectores públicos y semi-públicos sobre cómo garantizar el cumplimiento del Reglamento General de Protección de Datos de la Unión Europea
(Reglamento (UE) 2016/679)
Elaborado para el proyecto "T4DATA" financiado por la UE
(Acuerdo de subvención número: 769100 — T4DATA — REC-DATA-2016/REC-DATA-2016-01)
por
Douwe Korff
Profesor Emérito de Derecho Internacional, London Metropolitan University
Profesor Asociado Oxford Martin School, Universidad de Oxford
&
Marie Georges
Experta internacional europea en protección de datos (CNIL, EU, Consejo de Europo, etc.)
Miembros del Grupo de Expertos Europeos de Derechos Fundamentales (Fundamental Rights Experts Europe - FREE)
Aprovechando las principales contribuciones de la Agencia Italiana de Protección de Datos & los socios del proyecto
Aprobado por la Comisión, julio de 2019

https://www.aepd.es/sites/default/files/2019-12/El%20Manual%20del%20DPD%20-%20KORFFGEORGES%20-%20ESP.pdf

¿Cómo cumplo?

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Preguntas

- ¿Dónde están los datos que almacena la empresa?
- ¿Por qué se almacenan estos datos?
- ¿Tienes el consentimiento de tus consumidores?
- ¿Quién tiene acceso a estos datos?
- ¿Quién los tramita?
- ¿Cuánto tiempo los guardas?
- ¿Cómo los recoges?

Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

1. Identificar si se hace tratamiento de datos personales

RGPD Articulo 4 punto 2

«tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, 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;

Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

1. Identificar si se hace tratamiento de datos personales

REALIZAR UN INVENTARIO DE LOS DATOS y CLASIFICARLOS

Por criterios
- ✓ confidencialidad
- ✓ integridad
- ✓ disponibilidad

Por el impacto que ocasionaría su
- ✓ pérdida
- ✓ difusión
- ✓ acceso no autorizado
- ✓ destrucción o alteración

Por las consecuencias :
- ✓ daño de imagen
- ✓ consecuencias legales
- ✓ consecuencias económicas
- ✓ paralización de la actividad

Por su utilidad o funcionalidad:
- ✓ información de clientes y proveedores
- ✓ información de compras y ventas
- ✓ información de personal y gestión interna
- ✓ información sobre pedidos y procesos de almacén

Por ciclo de vida
- ✓ vida útil del soporte sino
- ✓ vigencia de su contenido

Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

2. Garantiza los derechos y libertades de los individuos con respecto a sus datos personales:

https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf

- informándoles de forma visible, accesible, sencilla y transparente sobre el tratamiento de sus datos;
- obteniendo de ellos el consentimiento inequívoco o expreso según las categorías del datos del tratamiento (No es válido el consentimiento tácito, es decir basado en inacción u omisión)
- permitiéndoles ejercitar sus derechos de forma sencilla, trasparente, y en los plazos previstos;
- notificándoles en caso de violaciones de seguridad que pudieran afectarles.

Informar	Obtener consentimiento	Garantizar derechos	Notificar violaciones
Tratamiento	Inequívoco	Que puedan ejercerlos	Que supongan riesgo para la privacidad
Decisiones automatizadas	No tácito	Según los plazos RGPD	A la autoridad
Perfiles	Expreso en caso de datos de especial protección		A los usuarios
Transferencias internacionales			

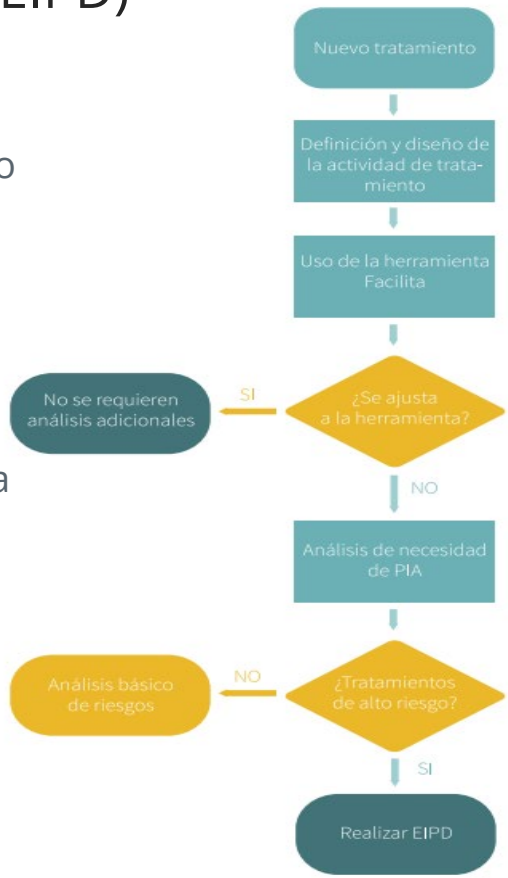
Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

3. Realiza una Gestión de Riesgos

Evaluación de Impacto en Protección de Datos (EIPD)
Privacy Impact Assessment (PIA)

- tratamientos de datos especialmente protegidos de forma sistemática o masiva;
- tratamientos de datos de forma masiva o *Big Data*;
- tratamientos de datos de menores de edad de forma significativa;
- el objetivo del tratamiento es predecir aspectos personales o elaborar perfiles;
- se cruzan datos de usuarios con los de otras fuentes;
- se utilizarán los datos obtenidos para una finalidad más intrusiva que la finalidad original para la que fueron recogidos;
- utilización de tecnologías especialmente invasivas para la privacidad;
- cesión de datos a terceros;
- transferencia de datos a países fuera del EEE (Espacio Económico Europeo);
- se contactará con las personas de forma intrusiva;
- utilización de datos personales no disociados o no anonimizados de forma irreversible para fines estadísticos, históricos o de investigación científica;
- riesgos específicos que puedan comprometer la confidencialidad, la integridad o la disponibilidad de los datos personales.



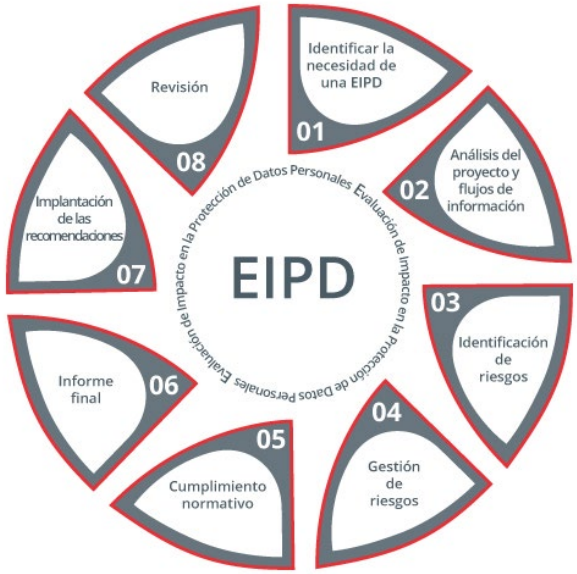
Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

3. Realiza una Gestión de Riesgos

- Una descripción sistemática de la actividad de tratamiento previstas
- Una evaluación de la necesidad y proporcionalidad del tratamiento respecto a su finalidad
- Una evaluación de los riesgos
- Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.



¿Quien debe hacer el EIPD?

El **Responsable del Tratamiento** con el asesoramiento del Delegado de Protección de Datos

FASE	Responsable del tratamiento	DPD	Encargado del tratamiento	Otras áreas relevantes (pe seguridad, riesgos, Asesoría Jurídica, ...)
1 Describir el ciclo de vida de los datos	R/A	C/I	C	C
2 Analizar la necesidad y proporcionalidad del tratamiento	R/A	C/I	C	C
3 Identificar amenazas y riesgos	R/A	C/I	C	-
4 Evaluar los riesgos	R/A	C/I	C	-
5 Tratar los riesgos	R/A	C/I	C	C
6 Plan de acción y conclusiones	R/A	C/I	C	C

Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

3. Realiza una Gestión de Riesgos

https://www.aepd.es/es/documento/guia-analisis-de-riesgos-rgpd.pdf

Tratamientos de bajo riesgo
(no son tratamientos masivos ni con datos especialmente protegidos)

RGPD FACILITA 2.0
HERRAMIENTA PARA TRATAMIENTOS DE ESCASO RIESGO

https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDMzNDAyNjMxNjE5NjIyODU2NTIy/?updated=true

Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

3. Realiza una Gestión de Riesgos

A) Identificar Amenazas

- Acceso ilegítimo a los datos

¿qué daño causaría que lo conociera quien no debe?

CONFIDENCIALIDAD

- Modificación no autorizada de los datos

¿qué perjuicio causaría que estuviera dañado o corrupto?

INTEGRIDAD

- Eliminación de los datos:

¿qué perjuicio causaría no tener un dato o no poder utilizarlo?

DISPONIBILIDAD

Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

3. Realiza una Gestión de Riesgos

B) Evaluación de Riesgos

OBJETIVO: Valorar y estimar la probabilidad y el impacto de que el riesgo se materialice

¿Qué es un Riesgo?

Riesgo = Probabilidad X Impacto

Un riesgo se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas. El nivel del riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo.

***Ejemplo**: La pérdida de un dispositivo móvil o la fuga de información (**Amenaza**), podría derivar en un acceso por parte de personal no autorizado a los datos y, en consecuencia, se produciría una vulneración de los derechos y libertades de los interesados (**Riesgo**), lo que podría derivar en un posible daño moral, físico o material sobre el interesado (**Impacto**).*

Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

3. Realiza una Gestión de Riesgos

B) Evaluación de Riesgos

Riesgo = Probabilidad X Impacto

Matriz de Riesgo

Probabilidad					
	Máxima 4	4	8	12	16
	Significativa 3	3	6	9	12
	Limitada 2	2	4	6	8
	Despreciable 1	1	2	3	4
		Despreciable · 1	Limitada · 2	Significativa · 3	Máxima · 4

Bajo
Medio
Alto
Muy Alto

IMPACTO

Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

3. Realiza una Gestión de Riesgos

Tipo amenaza	Amenaza	Riesgo	Probabilidad	Impacto	Riesgo inherente
Acceso ilegítimo a los datos	***Fuga de información*** *(derivada de la pérdida del* ***dispositivo móvil)***	*Acceso no autorizado por parte de terceros a datos de salud (violación de la confidencialidad)*	*Significativa* 3	*Significativo* 3	*Alto* 9
	Operación de tratamiento no autorizada *(derivada del uso de los datos para una finalidad sin base legitimadora, por ejemplo, acciones de marketing indirecto sobre productos de salud)*	*Uso ilegítimo de datos personales (vulneración de los derechos y libertades)*	*Máxima* 4	*Limitado* 2	*Alto* 8
Modificación no autorizada de los datos	***Ataque cibernético*** *(malware que modifica los datos almacenados en la nube)*	*Modificación de datos no autorizada por parte de terceros (violación de la integridad)*	*Significativa* 3	*Limitado* 2	*Medio* 6
	Operación de tratamiento no autorizada *(derivada de una* ***decisión automatizada en base al perfilado de datos*** *erróneo por una* ***mala programación del software****, por ejemplo, una categorización de personas saludables con acceso a determinadas coberturas de un seguro de salud)*	*Uso ilegítimo de datos personales (vulneración de los derechos y libertades)*	*Máxima* 4	*Significativo* 3	*Muy alto* 12
Eliminación de los datos	***Corte de suministro eléctrico o fallos en servicios de comunicaciones****(como consecuencia del fallo se produce un periodo temporal en el cual los datos no han sido almacenados)*	*Pérdida de datos almacenados en el sistema (violación de la disponibilidad)*	*Limitada* 2	*Limitado* 2	*Medio* 4
	Ataque intencionado que provoca la indisponibilidad de los datos *(como consecuencia de un ataque de cifrado de las bases de datos que inhabilita las mismas)*	*Pérdida de datos almacenados en el sistema (violación de la disponibilidad)*	*Significativa* 3	*Significativo* 3	*Alto* 9

Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

3. Realiza una Gestión de Riesgos

C) Tratar los Riesgos

OBJETIVO: disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto

Medidas para tratar el Riesgo:

- Reducción del Riesgo: Para reducir el nivel de riesgo, se deben establecer medidas de control que reduzcan los niveles de probabilidad y/o impacto asociados al riesgo inherente.
- Retención del Riesgo: Si el nivel de riesgo inherente es inferior al nivel de riesgo considerado como aceptable, no existe necesidad de implementar controles adicionales.
- Transferencia del Riesgo: Consiste en compartir un riesgo con una organización externa. Se puede transferir el riesgo a una aseguradora que afronte las posibles consecuencias materiales. Sin embargo, se ha de considerar que, en ocasiones, la transferencia de riesgos puede generar otros riesgos. Por ello, la transferencia puede generar la necesidad de análisis adicionales.
- Anulación del Riesgo: Si el riesgo es muy elevado y no se quiere asumir el mismo, se puede decidir abandonar la actividad de tratamiento.

Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

3. Realiza una Gestión de Riesgos

C) Tratar los Riesgos

OBJETIVO: disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto

Medidas de Control

- Organizativas: Medidas asociadas a procedimientos, a la organización y gobierno de la entidad. En esta tipología de medidas se pueden incluir los procedimientos para ejercer los derechos de los interesados, protocolos para gestionar vulnerabilidades e incidentes, etc.
- Legales: Medidas asociadas al cumplimiento normativo. Por ejemplo, cláusulas para recogida de consentimientos expresos, etc.
- Técnicas: Medidas que permiten velar por la seguridad física y lógica de los activos de información. Por ejemplo, controles de acceso, cifrado, etc.

Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

3. Realiza una Gestión de Riesgos

C) Tratar los Riesgos

OBJETIVO: disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto

Medidas de Control Técnicas

- Utilizar distintas soluciones de prevención de fuga de información que permitan monitorizar el uso de los datos, conocer quién accede, cuando se borran, etc
- 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 de datos.
- Realizar backups mediante instrumentos específicos de contingencia y continuidad.
- Instalar y activar herramientas anti-fraude y anti-malware.
- Proteger las redes y comunicaciones tanto por cable como inalámbricas con Cortafuegos, IDS/IPS, VPNs

Implementación de Medidas para el Cumplimiento del RGPD

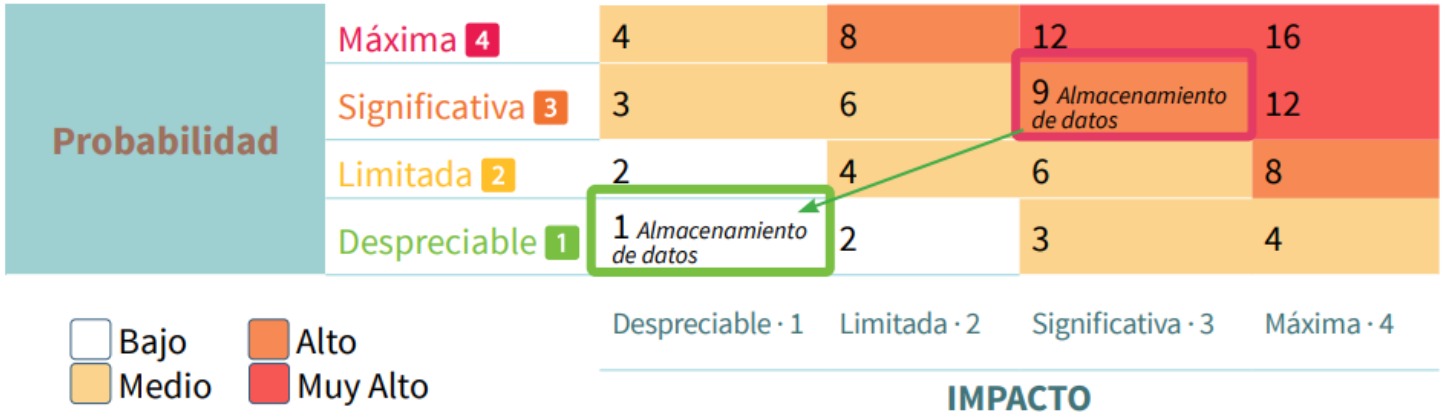
HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

3. Realiza una Gestión de Riesgos

C) Tratar los Riesgos

Riesgo residual = Probabilidad X Impacto

El **Riesgo Residual** es el riesgo de cada actividad una vez se hayan aplicado las medidas de control para mitigar y/o reducir su nivel de exposición



Implementación de Medidas para el Cumplimiento del RGPD

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

4. Revisa los contratos con los Encargados

- ❑ LAS INSTRUCCIONES DEL RESPONSABLE DEL TRATAMIENTO
- ❑ EL DEBER DE CONFIDENCIALIDAD
- ❑ LAS MEDIDAS DE SEGURIDAD
- ❑ EL RÉGIMEN DE LA SUBCONTRATACIÓN
- ❑ LOS DERECHOS DE LOS INTERESADOS
- ❑ LA COLABORACIÓN EN EL CUMPLIMIENTO DE LAS OBLIGACIONES DEL RESPONSABLE
- ❑ EL DESTINO DE LOS DATOS AL FINALIZAR LA PRESTACIÓN
- ❑ LA COLABORACIÓN CON EL RESPONSABLE PARA DEMOSTRAR EL CUMPLIMIENTO

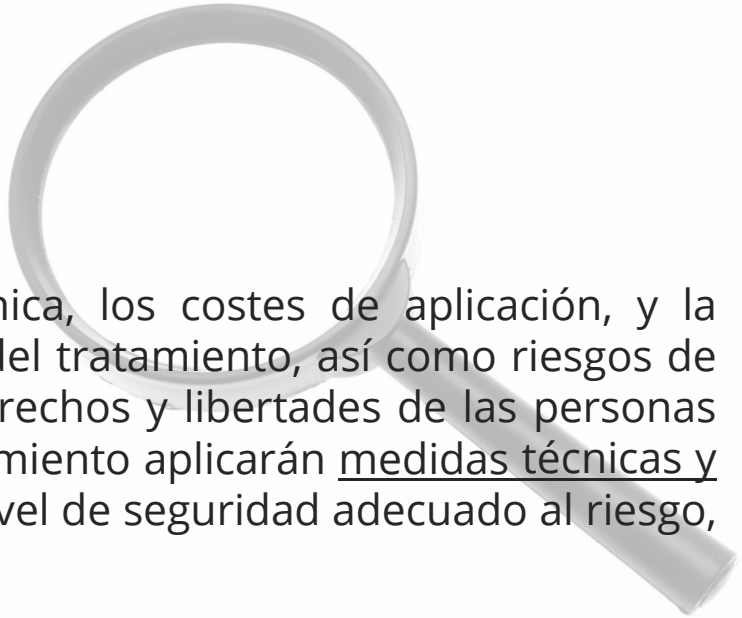
https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf

Necesidad de Realizar Auditorías Periódicas

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

¿Es necesario realizar auditorias periódicas?



Seguridad del Tratamiento
Artículo 32

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya (....)

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Necesidad de Realizar Auditorías Periódicas

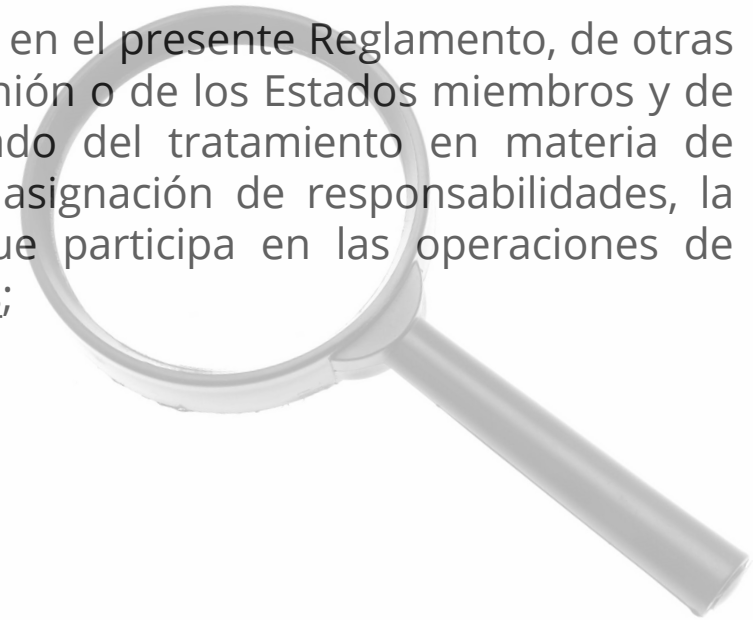
HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Funciones del Delegado de Protección de Datos

Artículo 39

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones (...)

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;



Necesidad de Realizar Auditorías Periódicas

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

¿

BOLETÍN OFICIAL DEL ESTADO
Núm. 294 Jueves 6 de diciembre de 2018 Sec. I. Pág. 119788

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

?

agencia española protección datos

Datuak Babesteko Euskal Bulegoa
Agencia Vasca de Protección de Datos

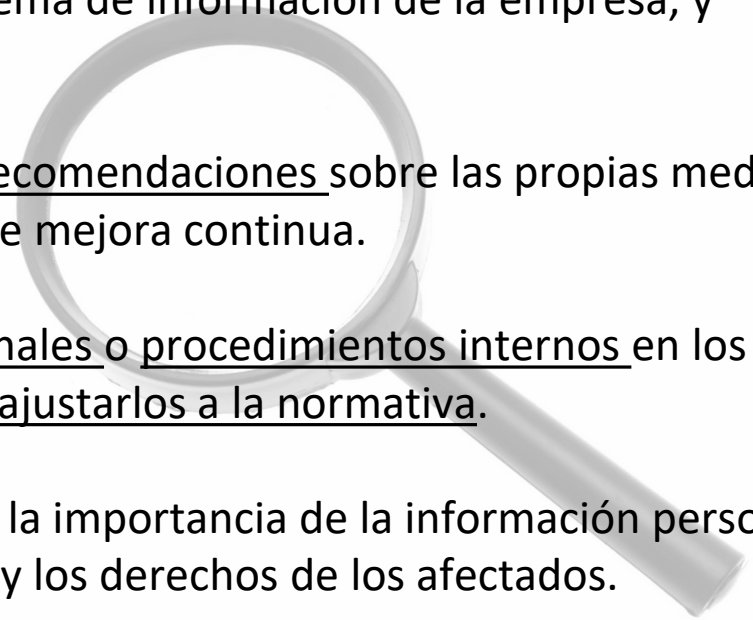
https://www.aepd.es/sites/default/files/2019-10/guia-directrices-contratos.pdf

Necesidad de Realizar Auditorías Periódicas

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

Objetivos de la Auditoria

- Satisfacer la obligación de verificar las medidas de seguridad.
- Constatar posibles deficiencias en el sistema de información de la empresa, y establecer acciones correctoras.
- Considerar oportunidades de mejora y recomendaciones sobre las propias medidas de seguridad auditadas, en un proceso de mejora continua.
- Estudiar en detalle flujos de datos personales o procedimientos internos en los que la RGPD tiene un especial impacto, para ajustarlos a la normativa.
- Concienciar y preparar al personal sobre la importancia de la información personal. Asegurando de esta forma la protección y los derechos de los afectados.



Conclusión.

HELPHONE
SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA

LA PROTECCIÓN DE DATOS PERSONALES DE TUS CLIENTES, USUARIOS, COLABORADORES O EMPLEADOS

RGPD

Evita las cuantiosas sanciones

+

Importante factor de competitividad y fidelización

MUCHAS GRACIAS
ESKERRIK ASKO

HELPHONE

SERVICIOS IT
ATENCIÓN AL CLIENTE
SERVICIOS DE INGENIERÍA
ASISTENCIA POSTVENTA


ESKERRIK ASKO
PARTE
HARTZEAGATIK
ingeniariak
GRACIAS POR
ASISTIR