S21SEC

Your Cybersecurity Company

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Reglamento Europeo de Protección de Datos

Julio 2018

WELCOME

The information provided in this document is the property of S21sec, and any modification or use of all or part of the content of this document without the express written consent of S21sec is strictly prohibited. Failure to reply to a request for consent shall in no case be understood as tacit authorisation for the use thereof.

© Grupo S21sec Gestión, S.A.

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

- Introducción y Conceptos Básicos
- Principales Novedades del RGPD
- Legislación Aplicable de Obligado Cumplimiento: Sanciones
- Deber de Información y Consentimiento de la persona interesada
- Medidas de Seguridad Aplicables
- Gestión de Soportes con Datos de Carácter Personal
- Derechos de los Interesados
- Conclusiones

INDEX

S21SEC
Your Cybersecurity Company

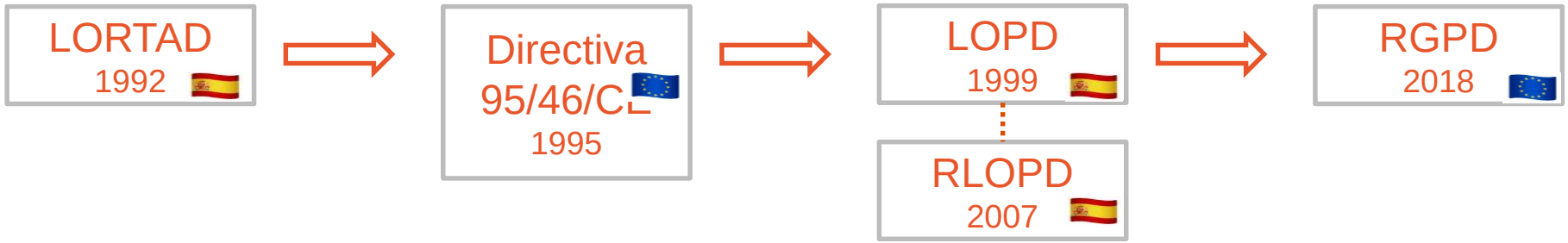
INTRODUCCIÓN Y CONCEPTOS BÁSICOS

S21SEC
Your Cybersecurity Company

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

¿QUÉ ES EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)?

- **Nuevo Reglamento Europeo RGPD (UE 2016/679): Aprobado el 27/04/2016**
- Se articula en **173 Considerandos Preliminares**, **11 Capítulos** y **99 Artículos**.
- **Entró en vigor el 25/05/2018.**



PRIVATE & CONFIDENTIAL

TIPOS DE DATOS

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

PRIVATE & CONFIDENTIAL

INTRODUCCIÓN Y OBJETIVOS

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

- **Una única normativa en toda la UE sobre Datos de Carácter Personal.**
- **Reforzar la Seguridad jurídica de personas físicas y operadores.**
- **Elevar la protección de los derechos de las personas físicas.**
- **Aumentar el control de la persona interesada sobre sus datos personales.**
- **Garantizar la libre circulación de datos dentro de la UE.**

CONCEPTOS BÁSICOS

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

- **Dato de Carácter Personal:** Toda la información sobre una persona física identificada o identificable, cuya identidad pueda ser determinada. Nombre, teléfono, dirección, foto, etc.
- **Tratamiento:** Cualquier operación realizada sobre un dato o un conjunto de datos, mediante procedimientos automatizados o no automatizados.
- **Finalidad:** Objeto por el cual han sido recogidos los datos y van a ser tratados. La finalidad debe ser clara y concisa y trasladarla a la ciudadanía en el momento de la recolección de los datos.

PRIVATE & CONFIDENTIAL

CONCEPTOS BÁSICOS

- **Responsable del Tratamiento:** La persona jurídica que define la finalidad y tratamiento que se realizará a los datos y se responsabiliza de su custodia y protección durante el tiempo destinado al tratamiento.
- **Encargado/a de Tratamiento:** La persona jurídica que realizará tratamiento a los datos por cuenta de la persona responsable durante un período de tiempo estipulado bajo contrato.
- **Autoridad de Control:** Autoridad pública, independiente, establecida por el estado, para controlar la correcta implantación del RGPD

PRIVATE & CONFIDENTIAL

CONCEPTOS BÁSICOS

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Principio de Responsabilidad Proactiva:

El RGPD describe este principio como **la necesidad** de que la o el responsable del tratamiento aplique **medidas técnicas y organizativas apropiadas** a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

En términos prácticos, este principio requiere que las organizaciones analicen **qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo..**

Este principio exige una **actitud consciente, diligente y proactiva** por parte de las organizaciones.

PRINCIPALES NOVEDADES DEL RGPD

S21SEC
Your Cybersecurity Company

PRINCIPALES NOVEDADES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

En cuanto a las empresas que deben cumplir el Reglamento, **se amplía el ámbito de aplicación a aquellas empresas no establecidas en la Unión Europea que realicen tratamientos** derivados de una oferta de bienes o servicios destinados **a personas ciudadanas de la Unión Europea** o como consecuencia de una monitorización y seguimiento de su comportamiento.

PRIVATE & CONFIDENTIAL

PRINCIPALES NOVEDADES

Se refuerza la **exigencia de consentimiento**, mediante una declaración o una acción positiva **no pudiendo deducirse del silencio o de la inacción**, estableciendo la **obligación de disponer de sistemas de registro del consentimiento**. Además se introduce la exigencia del consentimiento para la oferta directa a niñas/os de servicios de la sociedad de la información (internet), que será válido para mayores de 14 años, mientras que para menores de 14 años se necesitará el consentimiento de la madre/padre o tutor/a.

PRINCIPALES NOVEDADES

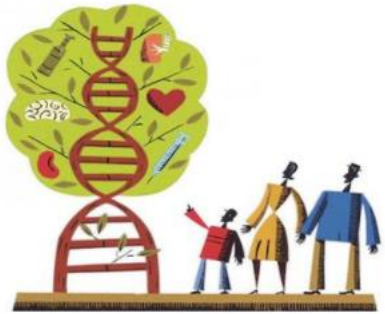
gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Se refuerza el **derecho de transparencia**, obligando a suministrar más información con carácter previo a la recogida de sus datos y el **derecho al olvido** para pedir que los datos personales sean suprimidos en determinadas circunstancias.

PRIVATE & CONFIDENTIAL

PRINCIPALES NOVEDADES

A los ya considerados como **datos especialmente protegidos** (ideología, religión, afiliación sindical, creencias, salud, origen racial y vida sexual) se añaden los **datos genéticos y biométricos** dirigidos a identificar de manera inequívoca a una persona.



PRIVATE & CONFIDENTIAL

PRINCIPALES NOVEDADES

Se establece la **protección de datos desde el diseño**, mediante la aplicación de medidas apropiadas al determinar los medios de tratamiento y en el momento mismo del tratamiento y la protección por defecto para que los datos personales no sean accesibles sin la intervención de la persona a un número indeterminado de personas físicas.

PRINCIPALES NOVEDADES

Se establece la **obligación de mantener un registro de tratamientos** por encargo de terceros en **empresas con más de 250 trabajadoras y trabajadores**, en tratamientos de datos que entrañen **riesgo para derechos y libertades**, en tratamiento de **datos especialmente protegidos** o en tratamientos de **datos relativos a condenas e infracciones penales.**

PRINCIPALES NOVEDADES

Se introduce la **obligación de notificación a la Agencia Española de Protección de Datos y a la persona interesada aquellas brechas de seguridad** que se produzcan y que supongan riesgo de daños y perjuicios físicos, materiales o inmateriales para las personas físicas.

PRINCIPALES NOVEDADES

Se impone la obligación de **realizar evaluaciones de impacto** en protección de datos (EIPD), siempre que sea probable que las operaciones de tratamiento, especialmente cuando se utilicen nuevas tecnologías, entrañen un alto riesgo para los derechos y libertades de las personas físicas. **La Agencia Española de Protección de Datos publicará listas de los tipos de operaciones de tratamiento que requieran una evaluación de impacto**.

PRIVATE & CONFIDENTIAL

PRINCIPALES NOVEDADES

Se impone la obligación de nombrar una persona **delegada de protección de datos (DPO)** cuando los tratamientos se lleven a cabo por **autoridades y organismos públicos** (excepto los tribunales), cuando las actividades principales requieran **observación habitual y sistemática de personas interesadas a gran escala** o cuando consistan en el tratamiento **a gran escala de datos especialmente protegidos o relativos a condenas e infracciones penales**.

PRINCIPALES NOVEDADES

Se establece un sistema de **ventanilla única** para que los y las responsables establecidas en varios Estados miembros de la Unión Europea o que, estando en un solo Estado miembro, hagan tratamientos que afecten significativamente a ciudadanas y ciudadanos en varios Estados de la Unión Europea tengan **una única Autoridad de protección de datos como interlocutora**.

Se crea el **Comité Europeo de Protección de Datos** que sustituye al Grupo de trabajo del artículo 29 de la Directiva 95/46/CE

LEGISLACIÓN APLICABLE DE OBLIGADO CUMPLIMIENTO SANCIONES

S21SEC
Your Cybersecurity Company

SANCIONES

Se prevén **poderes para sancionar** con una advertencia, apercibimiento, solicitud de atención de ejercicio de derechos, limitaciones del tratamiento, y multas administrativas para las que se contempla un importante aumento de **las cuantías** que pueden llegar hasta los **20.000.000 o un 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior**, optándose por la de mayor cuantía. Se prevé que para el 25 de mayo de 2018 los Estados miembros comuniquen a la Comisión otras sanciones efectivas, proporcionadas y disuasorias que decidan aplicar para las infracciones que no estén sancionadas con multas administrativas en el Reglamento.

SANCIONES

- Las sanciones se clasifican de acuerdo a:
- Naturaleza, gravedad y duración (números afectados, nivel de los daños, perjuicios, etc. …)
- Medidas adoptadas para paliar los daños
- Intencionalidad o negligencia
- Grado de responsabilidad, habida cuenta de las medidas técnicas / organizativas adoptadas.
- Infracciones anteriores.
- Categoría de los datos afectados.
- Adhesión a códigos de conducta.
- Etc. …

INFRACCIONES

- El proyecto de ley español propone una clasificación de las infracciones en 3 niveles:
- MUY GRAVES

  Prescriben a los 3 años
- GRAVES

  Prescriben a los 2 años
- LEVES

  Prescriben al año

PRIVATE & CONFIDENTIAL

INFRACCIONES MUY GRAVES

- Vulnerar los principios y garantías fundamentales
- Incumplir el principio de licitud del tratamiento
- No hay consentimiento o este no es válido (consentimiento informado, explícito)
- Utilizar datos para otras finalidades no contempladas en la recogida
- Tratamiento de datos de categorías especiales sin consentimiento o innecesariamente
- Tratamiento de condenas o infracciones sin base y/o autorización jurídica
- Tratamiento de infracciones y sanciones administrativas sin ser un órgano competente para ello o tener alguna ley que lo respalde

PRIVATE & CONFIDENTIAL

INFRACCIONES MUY GRAVES

- Omisión del deber de informar
- Vulneración del deber de confidencialidad
- Exigir un pago para facilitar el ejercicio de derechos
- No atender en plazo el ejercicio de derechos
- Incumple la obligación de bloqueo de datos
- Impedir el acceso por parte de la autoridad de protección de datos a información requerida

PRIVATE & CONFIDENTIAL

INFRACCIONES GRAVES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

- Tratamiento de datos de menores de edad sin consentimiento de su tutor/a
- No acreditar el esfuerzo razonable para verificar la validez del consentimiento de menores de edad
- Impedir, obstaculizar o no atender reiteradamente las solicitudes de ejercicio de derechos
- No aplicar medidas técnicas y organizativas apropiadas para garantizar que sólo se tratan los datos necesarios para cada finalidad
- No aplicar medidas técnicas y organizativas apropiadas para garantizar niveles de seguridad adecuados al riesgo del tratamiento

PRIVATE & CONFIDENTIAL

INFRACCIONES GRAVES

- Incumplir o quebrantar las medidas de seguridad impuestas
- No atender las solicitudes de las personas afectadas o de la autoridad de protección de datos
- No informar a la persona afectada de las violaciones de seguridad de sus datos
- No informar a la autoridad de protección de datos de las violaciones de seguridad de los datos

Entre otras…

PRIVATE & CONFIDENTIAL

INFRACCIONES LEVES

- Incumplir el principio de transparencia o derecho de información por no facilitar toda la información exigida
- Exigir un pago a la interesada para facilitar el deber de informar o atender cualquier derecho de la persona interesada
- No atender las solicitudes de ejercicio de derechos salvo que sea un Encargado de Tratamiento.
- No notificar la rectificación o supresión de datos o limitación del tratamiento
- No informar a la persona afectada, cuando lo haya solicitado, de la rectificación, supresión o limitaciones de tratamiento de datos en destinatarios/as de los mismos

INFRACCIONES LEVES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

- No suprimir los datos de una persona fallecida
- No formalizar con los/las corresponsables del tratamiento las obligaciones, funciones y responsabilidades
- Disponer de un registro de tratamientos incompleto
- Notificación incompleta de violaciones de seguridad a la autoridad de protección de datos
- Dar información inexacta a la autoridad de protección de datos cuando deba elevar una consulta

Entre otras…

PRIVATE & CONFIDENTIAL

DEBER DE INFORMACION Y CONSENTIMIENTO DE LA INTERESADA

S21SEC
Your Cybersecurity Company

DEBER DE INFORMACIÓN

Información que deberá facilitarse cuando los datos se obtengan de la persona interesada

1 Identidad y datos de contacto del o la responsable.

2 Datos de contacto del Delegad/a de Protección de Datos.

3 Fines del tratamiento.

4 Base Jurídica que legitima el tratamiento.

5 Intereses legítimos de la responsable (supuesto articulo 6.1.f).

6 Destinatarios o categoría de personas destinatarias.

7 En caso de Transferencia internacional de datos la existencia de decisión de adecuación del país o detalle de las garantías adecuadas utilizadas.

PRIVATE & CONFIDENTIAL

DEBER DE INFORMACIÓN

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Información que deberá facilitarse cuando los datos se obtengan de la persona interesada

8 Plazo de conservación de los datos.

9 Derechos de acceso, rectificación o supresión, oposición, limitación del tratamiento y portabilidad.

10 Derecho a reclamar ante Agencia de Protección de Datos.

11 Base jurídica para la comunicación de datos sin consentimiento (legal o contractual).

12 Obligación de prestar datos y consecuencias de no prestarlos.

PRIVATE & CONFIDENTIAL

DEBER DE INFORMACIÓN

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Información que deberá facilitarse cuando los datos se obtengan de la persona interesada

13 Si hay decisiones automatizadas, la lógica aplicada y consecuencias para la persona interesada.

14 Información sobre tratamientos posteriores de datos (momento previo a tratamiento posterior).

PRIVATE & CONFIDENTIAL

DEBER DE CONSENTIMIENTO

Condiciones para el Consentimiento:

- El o la responsable debe ser capaz de demostrar **consentimiento**, **de forma diferenciada** a otros asuntos.
- La solicitud debe ser **inteligible, de fácil acceso, de lenguaje sencillo y claro**.
- Si el tratamiento se basa en el mero consentimiento este **se podrá retirar fácilmente en cualquier momento**.
- Dentro de los contratos el consentimiento se podrá retirar para tratamientos no incluidos en el contrato.

DEBER DE CONSENTIMIENTO

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Consentimiento de menores en servicios de la sociedad de la Información:

- Cuando el tratamiento este basado en el consentimiento del o la menor, la responsable debe poner **medidas para verificar edad**.
- Edad mínima según ley aplicable **entre 13 a 16 años**, sino el consentimiento lo dará la persona que ejerce de tutora o representante.

PRIVATE & CONFIDENTIAL

DEBER DE CONSENTIMIENTO

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Recomendaciones de la Agencia respecto al consentimiento:

- **No seguir obteniendo consentimientos por omisión.**
- La adaptación puede llevarse a cabo:
  - Obteniendo un consentimiento de los interesados acorde con las disposiciones del RGPD.
  - Valorando si los tratamientos afectados pueden apoyarse en otra base legal como, el interés legítimo del responsable o del cesionario de los datos que prevalezca sobre los derechos del interesado.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

MEDIDAS DE SEGURIDAD APLICABLES

S21SEC
Your Cybersecurity Company

MEDIDAS DE SEGURIDAD APLICABLES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Medidas Técnicas

- El RGPD no enumera las medidas aplicables, como lo hacía la LOPD.
- Se traslada a las empresas la responsabilidad de definir las medidas de seguridad a aplicar.
- Las medidas de seguridad se definirán en función del resultado obtenido tras realizar un análisis de riesgo a cada uno de los tratamientos.
- Pueden definirse medidas estándar aplicables a todos los tratamientos, sin importar el tipo de datos que contengan o la finalidad de los mismos, como el control de acceso, copias de seguridad, registro de acceso (logs), gestión de incidentes de seguridad, etc.

PRIVATE & CONFIDENTIAL

MEDIDAS DE SEGURIDAD APLICABLES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Medidas Organizativas

- Las medidas organizativas o logísticas hacen referencia a las acciones cotidianas de la gestión de datos sensibles.
- Nombrar responsables y asignar roles a las personas involucradas en los tratamientos, con funciones específicas y controladas.
- Mantener la gestión y controlar las medidas técnicas establecidas y valorar aspectos jurídicos y legales de los tratamientos.
- Generar políticas de seguridad y trasladarlas a todo el personal para que haya un conocimiento generalizado de la gestión de datos personales.

PRIVATE & CONFIDENTIAL

GESTIÓN DE SOPORTES CON DATOS DE CARÁCTER PERSONAL

S21SEC
Your Cybersecurity Company

SOPORTES CON DATOS DE CARÁCTER PERSONAL

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Un soporte puede ser físico o lógico, digital o analógico, he aquí algunos ejemplos:

- Soporte Físico: Cualquier medio que pueda contener información.
  - Automatizada, en formato digital, pueden ser ordenadores, servidores, discos duros extraíbles, pendrives, teléfonos móviles, CDs, DVDs, Diskettes (si alguien aún los utiliza), cintas magnéticas de copias de seguridad, etc.
  - No automatizada, en formato papel, pueden ser libros, cuadernos, libretas, carpetas, post-its, tarjetas de visita, etc.
- Soporte lógico: Se refiere principalmente a datos almacenados en la nube, que son accesibles mediante soportes físicos, pero no se encuentran almacenados en los mismos.

GESTIÓN DE SOPORTES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Inventario y Registro

- Los soportes deben estar inventariados y, los digitales, a ser posible, cifrados para garantizar la seguridad de los datos almacenados.
- No conviene que se utilicen soportes que no sean de la empresa porque pueden contener virus o más información de la que se debería.
- Siempre que se asigne un soporte a una persona, debe constar en algún registro y conocer el tipo de datos que va a contener y su sensibilidad.
- Las medidas de seguridad aplicables a los soportes deberán ser definidas utilizando la mentalidad de “ponerse en el peor de los escenarios posibles”.

PRIVATE & CONFIDENTIAL

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Inventario y Registro

Los soportes no automatizados también deberán estar inventariados y, al no poder garantizar medidas tecnológicas para su securización, se deberán eliminar, mediante destrucción física (con una trituradora de papel, por ejemplo) cuando los datos contenidos hayan dejado de ser útiles para el propósito o la finalidad del tratamiento.

PRIVATE & CONFIDENTIAL

GESTIÓN DE SOPORTES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Traslado

El traslado de soportes debe hacerse de tal forma que no permita a agentes externos conocer el contenido de los mismos, registrando siempre la entrada y salida de soportes de las instalaciones de la entidad.

A modo de ejemplo:

- Pendrives con datos sensibles, que requieran especial protección, deberán ser cifrados para garantizar que no se pueda acceder a su contenido por parte de personas que no deberían conocerlo.
- Hojas de inscripción a talleres, deberán ser transportadas dentro de sobres opacos, cerrados y custodiados en todo momento.

DERECHOS DE LOS INTERESADOS

S21SEC
Your Cybersecurity Company

DERECHOS ARCO

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

La LOPD presentaba los derechos ARCO como los derechos que podían ejercer lxs ciudadanxs respecto a sus datos.

Acceso	Conocer qué tipos de datos tiene y trata cualquier responsable.
Rectificación	Corregir aquellos datos que fueran incorrectos o estuvieran desactualizados.
Cancelación	Eliminar (lógicamente) los datos de la persona para que no pudieran ser tratados en el futuro.
Oposición	La persona puede oponerse a ciertos tratamientos considerados no proporcionados o que atentaran contra su integridad.

PRIVATE & CONFIDENTIAL

DERECHOS ARCO

El RGPD introduce, además, derechos adicionales que cubren las necesidades que han surgido en los últimos años

Supresión	También conocido como “derecho al olvido”, consiste en eliminar los enlaces a aquellos datos de fuentes públicas virtuales (internet) para no figurar como resultado en ciertas búsquedas que puedan atentar contra su integridad.
Limitación del Tratamiento	Oponerse a ciertos tratamientos concretos sin perjuicio de otros tratamientos por parte del mismo responsable que considere apropiados.
Portabilidad	Obtener los datos de un/a responsable para transmitirlos a otro sin que haya impedimentos. La persona responsable que trata los datos originariamente deberá entregarlos en un formato de uso común, estructurado y de lectura mecánica para que el/la destinataria pueda acceder a ellos.

PRIVATE & CONFIDENTIAL

DERECHOS ARCO

El RGPD complementa el Derecho de Oposición establecido en la LOPD

Oposición y derechos relacionados con decisiones individuales automatizadas	Incluye, además, la posibilidad de oponerse a que sus datos sean utilizados para el estudio profundo y la elaboración de perfiles personales automatizados que puedan conllevar acciones que afecten jurídica o personalmente a la ciudadana.

PRIVATE & CONFIDENTIAL

DERECHO DE ACCESO

La persona interesada tendrá **derecho a obtener de la responsable** del tratamiento la siguiente información:

1 Fines del tratamiento.
2 Categorías de datos personales de que se trate.
3 Destinatarios o categorías de destinatarios (incluidos terceros países).
4 Plazo previsto de conservación de los datos o criterios utilizados para determinar este plazo.

PRIVATE & CONFIDENTIAL

ASPECTOS DESTACADOS: DERECHOS DE LA PERSONA INTERESADA

La persona responsable del tratamiento **comunicará cualquier rectificación, supresión o limitación del tratamiento a cada persona destinataria** a quienes se hayan comunicado los datos previamente **salvo que sea imposible o exija un esfuerzo desproporcionado.**

La persona **responsable informará a la interesada** acerca de dichos destinatarios, si este así lo solicita.

DERECHO DE OPOSICIÓN

La persona interesada tendrá **derecho a oponerse al tratamiento de datos** por motivos relacionados con una situación particular en caso de datos recogidos en función de intereses o potestades publicas o intereses legítimos de la responsable. Esto **no será de aplicación si**:

- Existen **motivos legítimos** imperiosos que prevalezcan.
- Se mantiene para el ejercicio de **reclamaciones.**

DERECHO DE SUPRESIÓN (“Derecho al Olvido”)

La persona interesada tendrá derecho a obtener la supresión de los datos cuando concurra alguna de las circunstancias siguientes:

- Los datos personales **ya no sean necesarios** en relación con los fines originales o posteriores.
- La persona interesada **retire el consentimiento** para el tratamiento y este no se base en otro fundamento jurídico.
- La persona interesada **se oponga al tratamiento** basado en intereses legítimos o cuyo fin sea la mercadotecnia.
- …

PRIVATE & CONFIDENTIAL

DERECHO DE SUPRESIÓN (“Derecho al Olvido”)

- ….
- Los datos personales **hayan sido tratados ilícitamente.**
- Los datos personales deban suprimirse para el **cumplimiento de una obligación legal** de la responsable.

Cuando se deban suprimir los datos pero estos **se hayan hecho públicos** el responsable adoptará **medidas razonables** para informar a las responsables que estén tratando los datos personales **de la supresión de cualquier enlace a esos datos personales**, o cualquier copia o réplica de los mismos.

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

La persona interesada tendrá derecho a la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

- La persona interesada **impugne la exactitud** de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
- El tratamiento **sea ilícito** y la persona interesada solicite en lugar de la supresión, la limitación de su uso.
- …

DERECHO A LA LIMITACIÓN DEL TRATAMIENTO

- …
- **No se necesiten ya los datos pero la persona interesada los necesite** para la formulación, el ejercicio o la **defensa de reclamaciones**.
- La interesada se haya **opuesto al tratamiento mientras se verifica si los motivos legítimos** del responsable prevalecen sobre los de la interesada.

En caso de levantamiento de la limitación la interesada debe ser **informada** de ello previamente.

DERECHO A LA PORTABILIDAD

Derecho de la persona interesada a recibir los datos en un **formato estructurado**, de uso común y lectura mecánica, **y a transmitirlos a otro responsable** cuando :

- El tratamiento debe estar **basado en el consentimiento** de las personas interesadas (consentimiento para fines determinados, datos especiales o por contrato).
- El tratamiento se efectuará por **medios automatizados**.

PRIVATE & CONFIDENTIAL

DERECHO A LA PORTABILIDAD

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Si es técnicamente posible los datos se trasladarán **directamente** a la siguiente responsable.

El derecho de portabilidad **no es aplicable a tratamientos en interés publico** o en ejercicio de potestades publicas.

PRIVATE & CONFIDENTIAL

DECISIONES INDIVIDUALES AUTOMATIZADAS

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

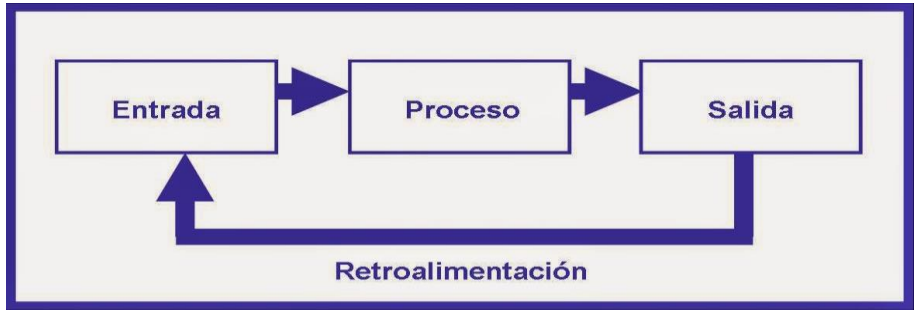
Derecho a **no ser objeto de una decisión únicamente automatizada (incluida elaboración de perfiles) Excepto**:

- Necesidad para ejecución de un contrato.
- Autorización por ley.
- Consentimiento explicito de la interesada.

DECISIONES INDIVIDUALES AUTOMATIZADAS

En todo caso el responsable garantizará a la persona interesada el **derecho a obtener intervención humana** por parte de la responsable, **a expresar su punto de vista y a impugnar la decisión**.

Las decisiones automatizadas **no se aplicarán sobre categorías de datos especiales salvo consentimiento expreso o interés publico**.



PRIVATE & CONFIDENTIAL

ASPECTOS DESTACADOS: DERECHOS DE LA PERSONA INTERESADA

- El o la responsable en el ejercicio de derechos facilitará **información concisa, transparente, inteligible en lenguaje claro y sencillo.**
- Se debe responder en un **plazo máximo de un mes** desde la recepción de la solicitud (3 meses si es compleja).
- Si el o la responsable **no da curso** a la solicitud **se informará en un mes de las razones** y de la posibilidad de reclamar ante autoridad de control y/o de ejercitar acciones judiciales.
- La comunicación de la información solicitada es **gratuita.**

ASPECTOS DESTACADOS: DERECHOS DEL INTERESADO

Todos estos derechos pueden ser ejercitados por la ciudadana en **cualquier momento**, durante el tratamiento de sus datos o posterior a la finalización del mismo; salvo que haya alguna base legal que prevalezca a los intereses particulares de la ciudadana, como pueden ser situaciones de la seguridad del Estado; defensa; seguridad pública; prevención, investigación, detección o enjuiciamiento de infracciones penales, etc.

CONCLUSIONES

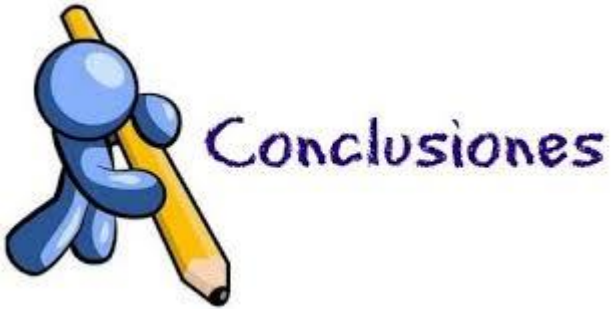
S21SEC
Your Cybersecurity Company

CONCLUSIONES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Nueva Normativa en materia de Protección de datos

- **Nuevo marco legal que entró en vigor en mayo de 2018.**
- **De obligado Cumplimiento.**
- **Aplicación en todo el ámbito de la UE y empresas que trabajen con datos de ciudadanxs de la UE.**



PRIVATE & CONFIDENTIAL

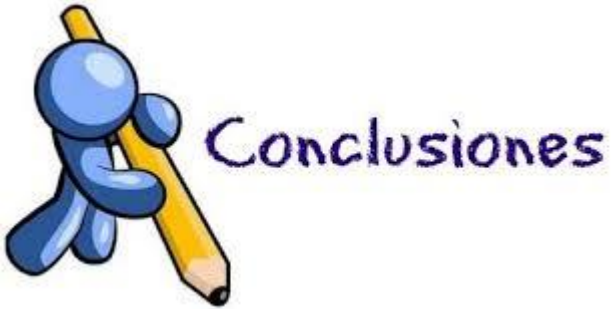
CONCLUSIONES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Responsabilidad Proactiva

- **No es suficiente con implantar medidas estáticas.**

- **Las medidas de seguridad que se implanten deben ser gestionadas y adaptarse a las diferentes situaciones que surjan.**



PRIVATE & CONFIDENTIAL

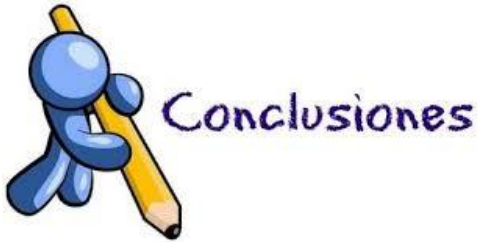
CONCLUSIONES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Enfoque orientado a los Riesgos

- **Las medidas de Seguridad que se adopten deben estar alineadas con el nivel de riesgo detectado.**

- **Deben ser coherentes con el valor de los datos protegidos y el impacto que la consecución del riesgo pueda producir: Realización de Análisis de Impacto.**



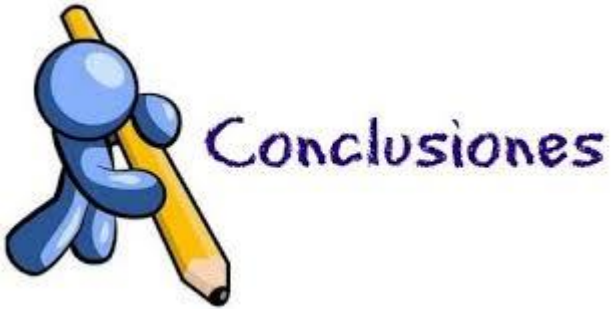
PRIVATE & CONFIDENTIAL

CONCLUSIONES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Notificación de Brechas de Seguridad

- **Se debe disponer de un procedimiento para notificar brechas de seguridad en los datos de carácter personal como a la AGPD.**



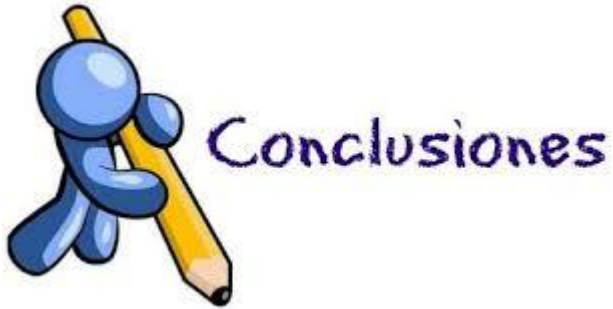
PRIVATE & CONFIDENTIAL

CONCLUSIONES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Nuevos derechos

- **Aparecen nuevos derechos de la ciudadanía, además de los ARCO, como el derecho al Olvido y el derecho a la Portabilidad.**



PRIVATE & CONFIDENTIAL

CONCLUSIONES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Consentimiento explícito

- **El consentimiento para el tratamiento de los datos por parte de las personas interesadas debe ser claro y explícito.**

- **No se acepta el consentimiento por omisión o silencio.**

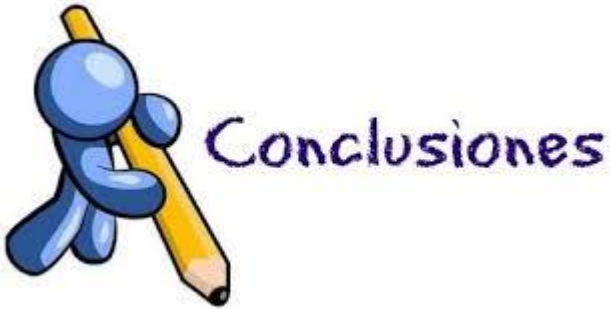
- **No se acepta el consentimiento obtenido de forma indirecta, encubierto en otros temas o con textos poco claros: Transparencia.**

CONCLUSIONES

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

Sanciones más altas

- **Aumenta considerablemente el importe de las sanciones respecto a la LOPD pudiendo llegar** hasta los **20.000.000 € o un 4% del volumen de negocio total anual global del ejercicio financiero anterior.**



PRIVATE & CONFIDENTIAL

gipuzkoa kutxa solidarioa
kutxa FUNDAZIOA

¿PREGUNTAS?

PRIVATE & CONFIDENTIAL

gipuzkoa
kutxa solidarioa
kutxa FUNDAZIOA

S21SEC

Your Cybersecurity Company

s21sec.com