Finanziaconnect

SCASSI. be secure

Reglamento General de Protección de Datos

Antonio Fernández

LOS DERECHOS QUE TIENES PARA PROTEGER TUS DATOS PERSONALES

EL 25 DE MAYO DE 2018 SE APLICA EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y ES IMPORTANTE QUE CONOZCAS CUÁLES SON TUS DERECHOS

1 DERECHO A CONOCER

- PARA QUÉ UTILIZAN TUS DATOS
  - Quién los tiene
  - Para qué los tienen
  - A quién los pueden ceder
  - Quiénes son sus destinatarios
- EL PLAZO DE CONSERVACIÓN DE TUS DATOS o Hasta cuándo van a ser utilizados
- QUE PUEDES PRESENTAR UNA RECLAMACIÓN ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
- LA EXISTENCIA DE DECISIONES AUTOMATIZADAS, LA ELABORACIÓN DE PERFILES Y SUS CONSECUENCIAS

2 DERECHO A SOLICITAR AL RESPONSABLE

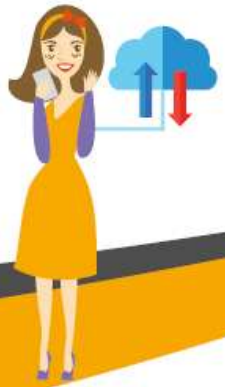
- LA SUSPENSIÓN DEL TRATAMIENTO DE TUS DATOS
  - Si impugnamos la exactitud de los datos, mientras se verifica dicha exactitud por parte del responsable
  - Si hemos ejercitado nuestro derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre tus derechos
- LA CONSERVACIÓN DE TUS DATOS
  - Si el tratamiento es ilícito y nos oponemos a la supresión de los datos solicitando la limitación de su uso
  - Si los datos se necesitan para la formulación, ejercicio o defensa de reclamaciones
- LA PORTABILIDAD DE TUS DATOS A OTROS PROVEEDORES DE SERVICIOS
  - En un formato estructurado, de uso común y lectura mecánica, siempre que sea técnicamente posible para su portabilidad y cuando los hayan utilizado/tratado con tu consentimiento o por existir un contrato

3 DERECHO A RECTIFICAR TUS DATOS

- CUANDO SEAN INEXACTOS
- CUANDO ESTÉN INCOMPLETOS

4 DERECHO A SUPRIMIR TUS DATOS

- POR TRATAMIENTO ILÍCITO DE DATOS
- POR LA DESAPARICIÓN DE LA FINALIDAD QUE MOTIVÓ EL TRATAMIENTO O RECOGIDA
- CUANDO REVOCAS TU CONSENTIMIENTO
- CUANDO TE OPONES A QUE SE TRATEN



5 DERECHO DE OPOSICIÓN AL TRATAMIENTO DE TUS DATOS

- POR MOTIVOS PERSONALES SALVO QUE QUIEN TRATA TUS DATOS ACREDITE UN INTERÉS LEGÍTIMO
- CUANDO EL TRATAMIENTO TENGA POR OBJETO EL MARKETING DIRECTO

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.agpd.es

Esta presentación contiene contenidos extraidos de la Agencia Española de Protección.
Estos datos están disponibles de forma pública
https://www.agpd.es

DERECHO A CONOCER* PARA QUÉ UTILIZAN TUS DATOS
· Quién los tiene
· Para qué los tienen
· A quién los pueden ceder
· Quiénes son sus destinatarios

* EL PLAZO DE CONSERVACIÓN DE TUS DATOS o Hasta cuándo vana ser utilizados

* QUE PUEDES PRESENTAR UNA RECLAMACIÓN ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

* LA EXISTENCIA DE DECISIONES AUTOMATIZADAS, LA ELABORACIÓN DE PERFILES Y SUS CONSECUENCIAS

DERECHO A SOLICITAR AL RESPONSABLE

* LA SUSPENSIÓN DEL TRATAMIENTO DE TUS DATOS

· Si impugnamos la exactitud de los datos, mientras se verifica dicha exactitud por parte del responsable

· Si hemos ejercitado nuestro derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre tus derechos

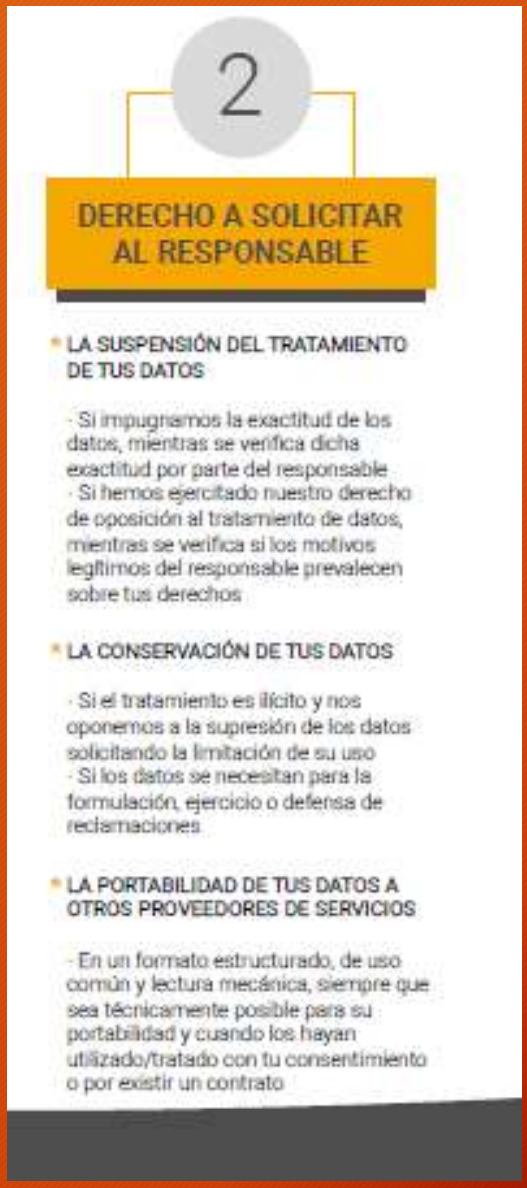
* LA CONSERVACIÓN DE TUS DATOS

· Si el tratamiento es ilícito y nos oponemos a la supresión de los datos solicitando la limitación de su uso

· Si los datos se necesitan para la formulación, ejercicio o defensa de reclamaciones

* LA PORTABILIDAD DE TUS DATOS A OTROS PROVEEDORES DE SERVICIOS

· En un formato estructurado, de uso común y lectura mecánica, siempre que sea técnicamente posible para su portabilidad y cuando los hayan utilizado/tratado con tu consentimiento o por existir un contrato



DERECHO A RECTIFICAR TUS DATOS

- CUANDO SEAN INEXACTOS
- CUANDO ESTÉN INCOMPLETOS

DERECHO A SUPRIMIR TUS DATOS

- POR TRATAMIENTO ILÍCITO DE DATOS
- POR LA DESAPARICIÓN DE LA FINALIDAD QUE MOTIVÓ EL TRATAMIENTO O RECOGIDA
- CUANDO REVOCAS TU CONSENTIMIENTO
- CUANDO TE OPONES A QUE SE TRATEN

DERECHO DE OPOSICIÓN AL TRATAMIENTO DE TUS DATOS

* POR MOTIVOS PERSONALES SALVO QUE QUIEN TRATA TUS DATOS ACREDITE UN INTERÉS LEGÍTIMO

* CUANDO EL TRATAMIENTO TENGA POR OBJETO EL MARKETING DIRECTO

¿Qué es un DPD?
(Delegado de protección de datos)

El Delegado de Protección de Datos es la persona que prestará ayuda y apoyo a los responsables de ficheros sobre el cumplimiento de la normativa.

¿Qué empresas deben nombrar un DPD?
(Delegado de protección de datos)

Administraciones públicas, organizaciones y empresas que cuenten con más de 250 trabajadores.

Empresas que, aunque tengan menos de 250 trabajadores, realicen tratamientos de datos a gran escala (lo que se conoce como fenómeno Big Data)

Entidades o empresas que manejen datos especialmente protegidos como son los datos de salud, religión, creencias, afiliación sindical o vida sexual. También se incluye el tratamiento de datos de localización o de menores.

Lista de verificación

Esta Lista de Verificación pretende ayudar a las organizaciones a llevar a cabo de forma ordenada una valoración de su situación frente a las principales obligaciones del RGPD

Legitimación

¿Tiene establecida claramente cuál es la base legal de los tratamientos que realiza y ha documentado de alguna forma el modo en que la ha establecido?

Si alguno de los tratamientos que realiza está basado en el consentimiento de los interesados, ¿ha verificado que ese consentimiento reúne los requisitos que exige el RGDP? En caso contrario, ¿ha previsto cómo recabar el consentimiento de forma adaptada al RGPD o ha encontrado otra base legal adecuada para esos tratamientos?

Información y derechos

La información que se proporciona a los interesados, ¿está presentada de forma clara, concisa, transparente y de fácil acceso?

¿Contiene esa información todos los elementos que prevé el RGPD?

¿Dispone de mecanismos para el ejercicio de derechos visibles, accesibles y sencillos? ¿Pueden ejercerse los derechos por vía electrónica?

¿Tiene establecidos procedimientos o mecanismos que le permitan verificar la identidad de quienes solicitan acceso o ejercen los demás derechos ARCO?

¿Tiene establecidos procedimientos que le permitan responder a los ejercicios de derechos en los plazos previstos por el RGPD? ¿Ha valorado si sería necesaria la colaboración de los encargados para responder a las solicitudes de los interesados y, si es así, tiene previsto incluir esta colaboración en los contratos de encargo?

En particular, ¿tiene previstos mecanismos para atender a posibles ejercicios del derecho a la limitación del tratamiento, de forma que los datos afectados puedan ser conservados sin ser objeto de las operaciones de tratamiento que corresponderían?

¿Ha valorado si los tratamientos de datos que realiza pueden ser objeto del derecho a la portabilidad? En caso, afirmativo, ¿ha previsto procedimientos o mecanismos para poder atender a este derecho y proporcionar los datos al interesado (o a otro responsable) en un formato estructurado, de uso común y susceptible de lectura mecánica?

Relaciones responsable-encargado

¿Ha previsto cómo valorar si los encargados con los que haya contratado o vaya a contratar operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD cuando sea de aplicación?

¿Contienen los contratos de encargo que actualmente tenga suscritos todos los elementos que prevé el RGPD? En caso contrario, ¿está dando pasos para adaptarlos antes de la aplicación del RGPD?

Medidas de responsabilidad proactiva

¿Ha hecho una valoración de los riesgos que los tratamientos que desarrolla implican para los derechos y libertades de los ciudadanos? ¿Ha determinado qué medidas de responsabilidad activa corresponden a su situación de riesgo y cómo debe aplicarlas?

¿Ha previsto cómo establecer el registro de actividades de tratamiento en su organización? ¿Ha valorado si le es de aplicación alguna de las excepciones a esta obligación? ¿Ha previsto quién se encargará de mantener actualizado el registro?

¿Ha revisado las medidas de seguridad que aplica a sus tratamientos a la luz de los resultados del análisis de riesgo de los mismos? ¿Considera que puede seguir aplicando las medidas de seguridad previstas en el Reglamento de la LOPD? ¿Ha valorado suficientemente la posibilidad de introducir medidas adicionales en función del tipo de tratamiento o del contexto en que se realiza?

Atendiendo al tipo de tratamientos que realiza, ¿ha establecido mecanismos para identificar con rapidez la existencia de violaciones de seguridad de los datos?

¿Tiene previstas medidas de reacción frente a los diferentes tipos de quiebras de seguridad, incluidos los procedimientos para evaluar el riesgo que puedan suponer para los derechos y libertades de los afectados?

¿Ha establecido procedimientos para notificar las violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados?

¿Dispone de un registro o herramienta similar en que pueda documentar los incidentes de seguridad que se produzcan, aunque no sean notificados a las autoridades de protección de datos?

¿Ha valorado si los tratamientos que realiza requieren una Evaluación de Impacto sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados?

¿Dispone de una metodología para la realización de la Evaluación de Impacto?

Según el tipo de tratamiento que realiza y los resultados del análisis de riesgos previo, ¿tiene que nombrar un Delegado de Protección de Datos?

¿Ha establecido los criterios para seleccionar al Delegado de Protección de Datos y, en particular, para valorar sus cualificaciones profesionales y sus conocimientos?

El puesto de DPD tal y como está configurado en su organización, ¿respeta los requisitos de independencia en el ejercicio de las funciones, posición en el organigrama, ausencia de conflicto de intereses y disponibilidad de los recursos necesarios establecidos por el RGPD?

¿Ha hecho pública la designación del DPD y sus datos de contacto y los ha comunicado a la autoridad de protección de datos?

¿Ha establecido procedimientos para que los interesados contacten con el DPD?

El principio de responsabilidad proactiva

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

¿Lo importante? que las medidas sean las adecuadas y que pueda **demostrarse**.

Personalización

"Al tener que definir de forma precisa el uso que se le van a dar a los datos recabados, debemos olvidarnos del cortar, pegar, sobre todo en formularios electrónicos. Esto implica el tener que modificar o crear de nuevo dichos formularios"

Formularios legales

Incluirán un check box donde el usuario debe aceptar el consentimiento de forma inequívoca y además, no puede estar marcado como opción por defecto.

Se debe introducir justo debajo del formulario los aspectos más significativos sobre el tratamiento que se va a dar a la información y en caso de ser necesario, se puede complementar con otra capa donde se complete toda la información necesaria.

Si optamos por esta formula, estaremos utilizando lo que la agencia de protección de datos denomina como información multinivel.

https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf

El conjunto de las informaciones requeridas por el RGPD pueden agruparse en unos
determinados epígrafes, a los efectos de su organización y presentación, especialmente en cuanto a la información a presentar, de forma resumida, en la primera capa o nivel

A partir de ahora , el RGPD añade requisitos adicionales en cuanto a la necesidad de informar a las personas interesadas, generalizando el concepto de "Tratamiento"incorporando, en líneas generales, los siguientes detalles:

- Los datos de contacto del Delegado de Protección de Datos, en su caso,
- La base jurídica o legitimación para el tratamiento,
- El plazo o los criterios de conservación de la información,
- La existencia de decisiones automatizadas o elaboración de perfiles,
- La previsión de transferencias a Terceros Países
- El derecho a presentar una reclamación ante las Autoridades de Control

Y además, en el caso de que los datos no se obtengan del propio interesado:

- El origen de los datos
- Las categorías de los datos

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

En consecuencia, los procedimientos, modelos o formularios diseñados de conformidad con la LOPD deberán ser revisados y adaptados por los Responsables de Tratamientos con anterioridad a la fecha de plena aplicación del RGPD, incorporando los nuevos requisitos que sean necesarios.

Puesto que los nuevos requisitos amplían y no contradicen la obligación de informar establecida en la LOPD, se recomienda revisar y aplicar dicha adaptación cuanto antes

Para mayor detalle pueden consultarse los artículos 13 y 14 del RGPD, relativos al
derecho de información de las personas interesadas.

http://www.privacy-regulation.eu/es/13.htm
http://www.privacy-regulation.eu/es/14.htm

¿Quién y cuándo debe informar?

La obligación de informar a las personas interesadas sobre las circunstancias relativas al tratamiento de sus datos recae sobre el Responsabledel Tratamiento.

La información se debe poner a disposición de los interesados en el momento en que se soliciten los datos, previamente a la recogida o registro, si es que los datos se obtienen directamente del interesado.

En el caso de que los datos no se obtengan del propio interesado, por proceder de alguna cesión legítima, o de fuentes de acceso público, el Responsable informará a

las personas interesadas dentro de un plazo razonable, pero en cualquier caso:

- antes de un mes desde que se obtuvieron los datos personales,
- antes o en la primera comunicación con el interesado
- antes de que los datos, en su caso, se hayan comunicado a otros destinatarios

Epígrafe	Información básica (1ª capa, resumida)	Información adicional (2ª capa, detallada)
"Responsable" (del tratamiento)	Identidad del Responsable del Tratamiento	Datos de contacto del Responsable
		Identidad y datos de contacto del representante
		Datos de contacto del Delegado de Protección de Datos
"Finalidad" (del tratamiento)	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento
		Plazos o criterios de conservación de los datos
		Decisiones automatizadas, perfiles y lógica aplicada
"Legitimación" (del tratamiento)	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.
		Obligación o no de facilitar datos y consecuencias de no hacerlo
"Destinatarios" (de cesiones o transferencias)	Previsión o no de Cesiones	Destinatarios o categorías de destinatarios
	Previsión de Transferencias, o no, a terceros países	Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables
"Derechos" (de las personas interesadas)	Referencia al ejercicio de derechos.	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento
		Derecho a retirar el consentimiento prestado
		Derecho a reclamar ante la Autoridad de Control
"Procedencia" (de los datos)	Fuente de los datos (cuando no proceden del interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público
		Categorías de datos que se traten

Ejemplo:

Nombre:

E- mail:

Consentimiento válido hasta:

☐ He leído y acepto la política de privacidad

EMPRESA FICTICIA le informa que los datos de carácter personal que nos proporcione cumplimentando este formulario, serán tratados por RESPONSABLE_DEL_SITIO que actúa como responsable de este sitio. La finalidad de la recogida y tratamiento de los datos personales que le solicitamos es para enviarle información de nuestro producto. La legitimación se realiza a través del consentimiento del interesado. le informamos que la información que nos facilitas se almacenara en los servidores de PROVEEDOR_DE_ALMACENAMIENTO que cumple todos los requisitos aprobados por el Comité Europeo de Protección de Datos. Puedes ver esta información aquí . Además puede comprobar su política de privacidad aquí . Para poder atender la demanda de este formulario es necesario que introduzca dichos datos, teniendo en cuenta que podrá ejercer sus derechos de acceso, rectificación, limitación y suprimir los datos en rgpd@empresaficticia.com así como el derecho a presentar una reclamación ante una autoridad de control. Si necesita algún tipo de información adicional, puede consultar nuestra política de privacidad.

Alguna de las medidas necesarias a implantar

- Cifrado de datos o seudonimización de los mismos (art. 4.5)
- Garantizar la confidencialidad, integridad y disponibilidad de forma continua
- Garantizar la resiliencia de forma continua

- Disponer de medidas para restaurar el acceso a los datos tras cualquier incidente
- Evaluar los sistemas de forma periódica con la realización de pruebas
- Políticas de uso responsable de la información y los recursos de la empresa
- Protocolos para el tratamiento de la información atendiendo a su confidencialidad
- Concienciación de los usuarios para evitar la pérdida de datos

Adaptar nuestros sistemas (Algunas recomendaciones)

- Debemos tener implementado un sistema de políticas para la gestión de la información
- Cifrado de discos
- Política de contraseñas
- Sistemas de copia de seguridad con pruebas periódicas
- Políticas de uso responsable que deberán ser firmadas por todos los empleados
- Tener un protocolo para catalogar la confidencialidad de la información que se maneja.
- Implementación del uso del puesto de trabajo seguro

Riesgos

Además, es importante registrar cada uno de los riesgos con sus posibles soluciones, así como el responsable de ponerlas en funcionamiento.

Esto quiere decir que es posible que necesitemos implantar algún tipo de registro electrónico para tal fin.

TABLA PARA ESTIMAR LA PROBABILIDAD	
VALOR	**DESCRIPCIÓN**
Bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Medio (2)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (3)	La amenaza se materializa a lo sumo una vez cada semana.

TABLA PARA ESTIMAR EL IMPACTO	
VALOR	**DESCRIPCIÓN**
Bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (2)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (3)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

CRITERIOS DE ACEPTACIÓN DEL RIESGO	
RANGO	**DESCRIPCIÓN**
Riesgo <= 4	La organización considera el riesgo poco reseñable.

Riesgos

Riesgos derivados del tratamiento que sean susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales como:

- La destrucción
- Pérdida o alteración accidental o ilícita de los datos personales en la transmisión, conservación o tratamiento
- La comunicación o accesos no autorizados a los datos

Riesgos

Elementos a proteger:

Discos duros (internos y externos).

- Cintas y discos de copias de seguridad.
- Unidades USB o *pendrives*.
- Tarjetas de memoria (SD, microSD, etc.)
- Discos ópticos (CD/DVD).

La mejor manera de proteger esta información es protegiendo estos soportes. Muy a menudo no hay un sistema definido ni medios implementados para que esta protección sea efectiva.

Riesgos

Cuando un dispositivo finaliza su vida útil:

Debemos disponer de un protocolo que no permita fugas de información

En muchas ocasiones necesitaremos adquirir medios

En muchas ocasiones hay que redactar por completo protocolos para realizarlo

Trazabilidad

Además de todo lo anterior, hay que registrar trazabilidad de las operaciones que se tengan que efectuar, por lo que también habrá de implementarse técnicamente algún tipo de solución.

Trazabilidad

Ejemplo típico: Cliente que quiere que se eliminen sus datos, solicita esto mismo y además quiere una prueba fehaciente de que se ha efectuado.

Pasado un tiempo el ya antiguo cliente, denuncia porque considera que no se han dado de baja sus datos tenemos una inspección donde se nos solicita un registro sobre el hecho denunciado.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Diferencias dependiendo de quien lo haga

Responsable del fichero
o
Encargado del tratamiento

- Identificación de responsable
- Fines del tratamiento.
- Descripción de categorías de interesados y datos.
- Categorías de destinatarios
- Transferencias internacionales de datos y documentación de garantías
- Plazos previstos para la supresión de datos
- Descripción de las medidas de seguridad

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

¿Cómo deben constar?

Siempre por escrito aunque también **se consideran válidos en formato electrónico**.

De cualquiera de las formas, siempre debe estar actualizado.

Implicaciones técnicas
En resumen, necesitamos adaptar nuestros sistemas

Adquisición de los datos

- Consentimiento
- Monitorización
- Seguimiento y control de cambios
- Autorización

Riesgos

- Afectados
- Corporativos
- Legales

Trazabilidad

- Hay que poder responder: Quien, Por qué, Para qué, Cuando, Donde

Implicaciones técnicas

Despliegue de medidas preventivas:

- Herramientas de reporting y auditoría
- Encriptación para asegurar la ilegibilidad de los datos
- Cifrado y control de accesos
- Monitorización
- Securización de dispositivos
- Protocolos de recuperación y validación de datos

Finanziaconnect

Preguntas y dudas

SCASSI
be secure