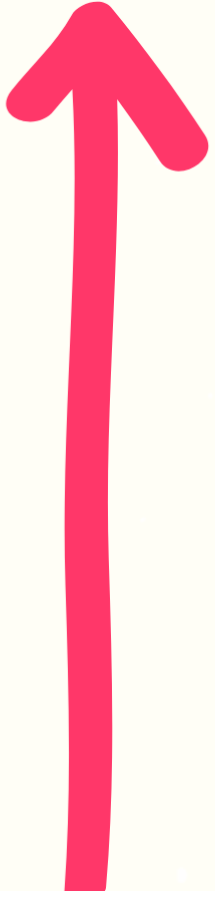
REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

mydonor
For social good

el RGPD contiene nuevas obligaciones y modifica ciertos aspectos del régimen actual.

Dos elementos constituyen la mayor innovación del RGPD: El principio de responsabilidad proactiva y el enfoque de riesgo

El consentimiento debe ser "inequívoco"



A diferencia del reglamento de Desarrollo de la LOPD, no se admiten formas de consentimiento tácito o por omisión, ya que se basan en la inacción.

El consentimiento puede ser inequívoco y otorgarse de forma implícita cuando se deduzca de una acción del interesado (por ejemplo, cuando el interesado acepta que se utilicen cookies).

Información de forma concisa, transparente, inteligible y de fácil acceso, con unlenguaje claro y sencillo. (La LOPD sólo exige
que la información se preste de modo expreso, preciso e inequívoco)

Derechos

Derecho al olvido

Es una manifestación de los derechos de cancelación u oposición en el entorno online.
(Borrado de los datos personales).

Limitación del tratamiento

A petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían.

Portabilidad

Implica que los datos personales del interesado se transmiten directamente de un responsable a otro, siempre que sea técnicamente posible.

Derecho de acceso

ANTES Debían facilitarse todos los datos de base del afectado, pero no copias o documentos (excepto en el caso de la historia clínica).

AHORA Se reconoce el derecho a obtener una copia de los datos personales objeto del tratamiento.

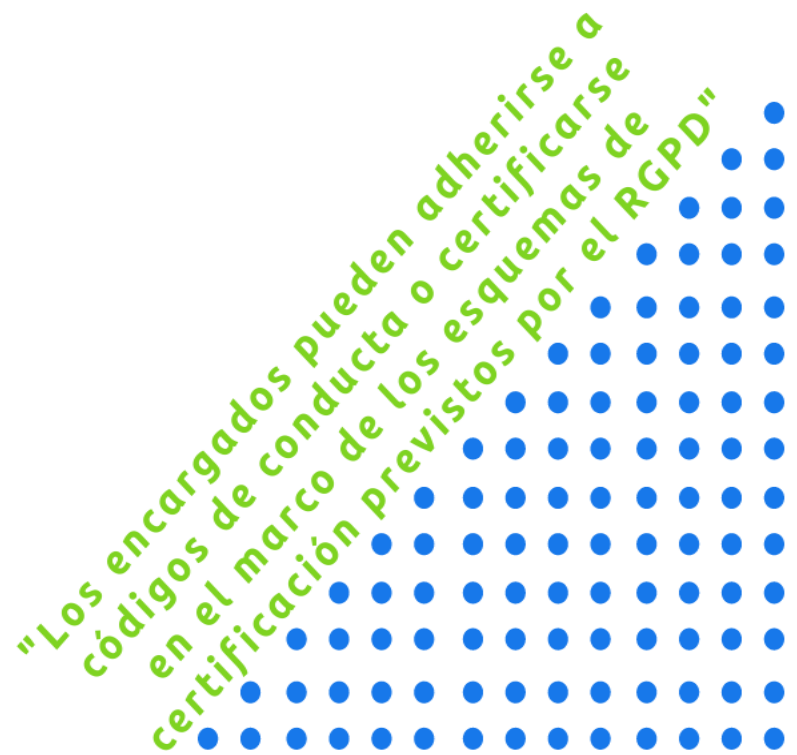
Se puede facilitar el acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales.

myDonor For social good

Obligaciones de los encargados

En determinadas materias los encargados tienen obligaciones propias que establece el RGPD, que no se circunscriben al ámbito del contrato que los une al responsable, y que pueden ser supervisadas separadamente por las autoridades de protección de datos:

- Deben mantener un registro de actividades de tratamiento.
- Deben determinar las medidas de seguridad aplicables a los tratamientos que realizan.
- Deben designar a un Delegado de Protección de datos en los casos previstos por el RGPD.



Responsabilidad activa

Análisis de riesgo

Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo hacerlo.

mydonor®

Análisis de riesgo

El tipo de análisis variará en función de:

- Los tipos de tratamiento
- La naturaleza de los datos
- El número de interesados afectados
- La cantidad y variedad de tratamientos que una misma organización lleve a cabo.

Análisis de riesgo

mydonor
For social good

Organizacionesde menor tamaño y de poca complejidad

El análisis será el resultado de una reflexión de una serie de preguntas, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados que al final llevará al tipo de tratamiento a seguir.

Grandes organizaciones

Como regla general, el análisis deberá llevarse a cabo utilizando alguna de las metodologías de análisis de riesgo existentes.

CUESTIONARIO EMPRESAS PEQUEÑAS!

Cuanto mayor sea el número de respuestas afirmativas mayor sería el riesgo que podría derivarse del tratamiento

¿Setratan datos sensibles?
¿Se incluyen datos de una gran cantidad de personas?
¿Incluye el tratamiento la elaboración de perfiles?
¿Se cruzan los datos obtenidos de los interesados con otros disponibles en otras fuentes?
Se pretende utilizar los datos obtenidos para una finalidad para otro tipo de finalidades?
¿Se están tratando grandes cantidades de datos, incluido con técnicas de análisis masivo tipo big data?
¿Se utilizan tecnologías especialmente invasivas para la privacidad, como las relativas a geolocalización, videovigilancia a gran escala o ciertas aplicaciones del Internet de las cosas?.

Registro de tratamiento

Responsables y encargados deberán mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD y que contenga cuestiones como:

- Nombre y datos de contacto del responsable o corresponsable y del Delegado de Protección de Datos si existiese
- Finalidades del tratamiento
- Descripción de categorías de interesados y categorías de datos personales tratados
- Transferencias internacionales de datos

Medidas de seguridad

myDonor
For social good

Antes	Ahora
El RGPD pide que se tomen en consideración más variables. El Reglamento de Desarrollo de la LOPD determinaba con detalle y de forma exhaustiva las medidas de seguridad que debían aplicarse según el tipo de datos objeto de tratamiento.	En el RGPD, los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo
Las medidas del Reglamento de la LOPD estaban basadas casi exclusivamente en el tipo de datos que se trataban, con alguna matización relativa al contexto en que se llevaban a cabo los tratamientos.	El RGPD pide que se tomen en consideración más variables.

violaciones de seguridad

El RGPD define las violaciones de seguridad de los datos, más comúnmente conocidas como **“quiebras de seguridad”**, de una forma muy amplia, que incluye todo incidente que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

- Cuando se produzca una violación de la seguridad de los datos, el responsable debe notificarla a la autoridad de protección de datos competente, a menos que sea improbable que la violación suponga un riesgo para los derechos y libertades de los afectados.
- La notificación de la quiebra a las autoridades debe producirse sin dilación indebida y, a ser posible, dentro de las 72 horas siguientes a que el responsable tenga constancia de ella.
- La notificación ha de incluir un contenido mínimo: la naturaleza de la violación; categorías de datos y de interesados; afectados; medidas adoptadas por el responsable para solventar la quiebra; si procede, las medidas aplicadas para paliar los posibles efectos negativos sobre los interesados.

Evaluación de impacto

Los responsables de tratamiento deberán realizar una **Evaluación de Impacto sobre la Protección de Datos (EIPD)** con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados.

Cuando el análisis de riesgo que las organizaciones lleven a cabo sobre los tratamientos iniciados con anterioridad a la fecha de aplicación del **RGPD** indiquen que esos **tratamientos presentan alto riesgo para los derechos o libertades de los interesados**, los responsables deberán realizar una EIPD sobre esos tratamientos, a fin de estar en condiciones de poder adoptar las medidas adecuadas para adecuar esos tratamientos a las exigencias del RGPD.

1

Análisis de necesidad

Valoración de la conveniencia de llevar a cabo o no una Evaluación de Impacto

2

Descripción del proyecto y de los flujos de información

Análisis en profundidad del proyecto obteniendo el detalle de las categorías de datos que se tratan

3

Identificación de los riesgos

Análisis de los posibles riesgos para la protección de datos de los afectados y valoración de la probabilidad de que sucedan

Decisión sobre las recomendaciones y las acciones que deben llevarse a cabo. Asignación de los recursos necesarios para su ejecución y del responsable de implantarlas.

1

Gestión de los riesgos identificados

Determinación de los controles y las medidas que han de adoptarse para eliminar, mitigar, transferir o aceptar los riesgos detectados.

2

Análisis de cumplimiento normativo

Verificación de que el producto o servicio que se está desarrollando cumple con los requerimientos en materia de protección de datos.

3

Informe final

Relación detallada de los riesgos identificados y de las recomendaciones y propuestas para eliminarlos o mitigarlos. Su destinatario principal es la dirección de la organización.

Análisis del resultado final para comprobar la efectividad de la EIPD y verificar si se han creado nuevos riesgos o se han detectado otros que habían pasado desapercibidos.

myDonor® For social good