MEMORIA DESCRIPTIVA DE LA SOLICITUD DE LA FUNDACIÓN PRO BONO ESPAÑA AL PREMIO A LA PROACTIVIDAD Y BUENAS PRÁCTICAS EN EL CUMPLIMIENTO DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y A LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES

ÍNDICE DE DOCUMENTOS:

Programa informativo de los talleres (enlace)

Taller 1. Registro de Actividades del Tratamiento (enlace)

- Presentación utilizada en la sesión, que se puede visualizar en este enlace.
- Instrucciones para completar el RAT, cuyo modelo facilitado se encuentra disponible en la web.

Taller 2. Cómo redactar una política o cláusula informativa de privacidad (enlace)

- Presentación utilizada en la sesión, que se puede visualizar en este enlace.
- Instrucciones para completar los siguientes modelos (todos disponibles en la web):
    - Modelo política de privacidad
    - Modelos primera capa informativa
    - Modelo cláusula de los firmantes
    - Modelo cláusula informativa trabajadores

Taller 3. Ejercicio de derechos de los afectados (enlace)

- Presentación utilizada en la sesión, que se puede visualizar en este enlace.
- Instrucciones para completar la política para el ejercicio de derechos cuyo modelo se encuentra disponible en la web.

Taller 4. Cómo identificar los encargados de tratamiento y preparar un contrato (enlace)

- Presentación utilizada en la sesión, que se puede visualizar en este enlace.
- Caso práctico sobre un contrato con encargado de tratamiento.
- Checklist para elegir proveedores.
- Como materiales complementarios disponibles en la web: las directrices de la AEPD para la elaboración de contratos y el modelo aprobado por la Comisión Europea.

Taller 5. Adaptación de páginas web (enlace)

- Presentación utilizada en la sesión, que se puede visualizar en este enlace.
- Instrucciones para completar los siguientes modelos (todos disponibles en la web):
    - Modelo de política de cookies
    - Modelo de banner y panel de configuración de cookies
    - Modelo de aviso legal y condiciones generales de uso y venta

Taller 6. Otras situaciones conflictivas comunes. Envío de newsletters y comunicaciones comerciales. Nombramiento del DPO (enlace)

- Presentación utilizada en la sesión, que se puede visualizar en este enlace.
- Instrucciones para completar el informe sobre la necesidad de nombrar un DPO, cuyo modelo facilitado se encuentra disponible en la web.

Taller 7. Herramientas gratuitas para ayudar al cumplimiento de la normativa de PD (enlace)

- Presentación utilizada en las sesiones, que se puede visualizar en este enlace y en este otro.
- Instrucciones para la utilización de las herramientas gratuitas de la AEPD para el cumplimiento en materia de protección de datos.
- Documentación generada por la herramienta FACILITA (que se encuentra disponible en la web).

Modelo de diploma otorgado a los asistentes

Abogados y abogadas responsables de los talleres (enlace)

Compendio de opiniones de los participantes en el programa Modo dataprotectiON

TALLERES FORMATIVOS GRATUITOS PARA ENTIDADES SIN ÁNIMO DE LUCRO

modo dataprotectiON

Las herramientas clave para las organizaciones del tercer sector en materia de Protección de Datos

ENLACE DE INSCRIPCIÓN

FORMACIÓN IMPARTIDA POR:

CLIFFORD CHANCE

Pérez-Llorca

Pinsent Masons

Ramón y Cajal ABOGADOS

UNA INICIATIVA DE:

Coordinadora de ONG para el Desarrollo Región de Murcia

www.coordinadoraongdrm.org

Fundación Pro Bono España

www.probonoespana.org

CON EL APOYO DE:

Región de Murcia

PRESENTACIÓN

La iniciativa “Modo dataprotectiON” es un programa formativo en el que a lo largo de siete talleres (cada uno de ellos compuesto por una sesión teórica y una práctica) varios abogados especializados contarán los aspectos teóricos de la normativa y facilitarán modelos y documentos para que cada entidad pueda trabajar internamente para cumplir con su misión de conformidad con la regulación en materia de protección de datos.

Esta formación online y gratuita es una herramienta esencial para la profesionalización de las ONG y ONGD de toda España. Antes de asistir a los talleres, te recomendamos visualizar las dos sesiones preliminares disponibles en **ESTA WEB.**

¿Quién la imparte? abogados y abogadas con gran experiencia en el área de protección de datos: Clifford Chance, Pérez Llorca, Pinsent Masons y Ramón y Cajal.

Las personas que asistan, al menos, al 60% de las sesiones podrán solicitar un certificado de participación firmado por la Coordinadora de ONGD de la Región de Murcia y la Fundación Pro Bono España..

¿QUÉ TENDRÁS QUE HACER?

1. Asistir a las sesiones programadas. *Aunque se quedarán grabadas para verlas todas las veces que sea necesario, siempre se recomienda asistir en directo, así conocerás la situación de otras entidades y podrás plantear las dudas que surjan durante la explicación.*
2. Poner en práctica la plantilla/modelo/práctica que se haya estudiado en el taller. *Para esto se han programado las dos sesiones de cada taller con un margen de 15 días.*
3. Asistir a la segunda sesión para compartir la experiencia, plantear dudas o comentar problemas surgidos y formas de resolverlos.

INSCRIPCIONES

Pincha AQUÍ para acceder al formulario de inscripción.

Requisitos:

1. Para participar en la formación debes: inscribirte en nombre de alguna entidad sin ánimo de lucro (como personal contratado o voluntario).
2. Recomendamos que la personas que se inscriba asuma las tareas relacionadas con el cumplimiento de la normativa de protección de datos en su entidad.
3. ¡Aprovechar la formación todo lo posible!

Para cualquier duda contacta con el equipo en : **mododataprotection@gmail.com**

Estos talleres no suponen ningún tipo de asesoramiento jurídico por parte de los y las profesionales del derecho que participan en los mismos, sino que están enfocados, únicamente, a difundir conocimientos generales en torno a la normativa de protección de datos para que las entidades sin ánimo de lucro conozcan las herramientas con las que desarrollar sus propios documentos internos.

AGENDA

Horario de todos los talleres: de 17h a 18.30h

Taller 1. Registro de actividades de tratamiento

El primer paso para cumplir con la normativa en protección de datos es elaborar y mantener actualizado el Registro de Actividades de Tratamiento, que contendrá toda la información sobre los datos de carácter personal de los que somos responsables y al que podrá acceder la Agencia Española de Protección de Datos. En este taller te enseñaremos cómo hacerlo.

Sesiones

1ª: 20 enero

2ª: 3 febrero

Taller 2. Cómo redactar una política o cláusula informativa de privacidad

La implementación de un sistema de protección de datos pasa por documentar todas las medidas adoptadas por la organización, facilitar su consulta y contar con los permisos y bases de legitimación necesarios. En este taller te ayudaremos a redactar toda esa documentación para cumplir con la normativa.

Sesiones

1ª: 10 febrero

2ª: 24 febrero

Taller 3. Ejercicio de derechos de los afectados

En este taller abordaremos cuestiones como ¿qué derechos tienen los titulares de los datos que manejamos? ¿Qué canales debemos habilitar para que puedan ejercerlos? ¿Cuáles son los pasos que debemos dar ante una reclamación de derechos y de qué plazos disponemos para responder?

Sesiones

1ª: 3 marzo

2ª: 17 marzo

Taller 4. Cómo identificar los encargados de tratamiento y preparar un contrato

En ocasiones, debemos permitir que terceros ajenos a nuestra organización accedan a datos de los que somos responsables (proveedores, gestorías, asesorías, etc.). En este taller veremos qué son los denominados “encargados de tratamiento” y qué obligaciones implican para nuestra organización.

Sesiones

1ª: 24 marzo

2ª: 7 abril

Taller 5. Adaptación de páginas web

La página web es nuestra carta de presentación y es importante que refleje nuestro compromiso con el cumplimiento normativo. En este taller conocerás cuáles son los textos legales que debes incluir en ella y te ayudaremos a elaborarlos.

Sesiones

1ª: 28 abril

2ª: 12 mayo

Taller 6. Otras situaciones conflictivas comunes. Envío de newsletters y comunicaciones comerciales. Nombramiento del DPO.

En este taller daremos respuesta a alguna de las dudas más recurrentes en materia de protección de datos: ¿a quién puedo enviar comunicaciones comerciales o promocionales y cómo debo hacerlo? ¿ Está obligada mi organización a contar con un delegado de protección de datos? ¿Qué requisitos debe cumplir?

Sesiones

1ª: 19 mayo

2ª: 2 junio

Taller 7. Herramientas gratuitas para ayudar al cumplimiento de la normativa de PD

La propia Agencia Española de Protección de Datos cuenta con recursos de acceso gratuito para facilitar la implementación del sistema de protección de datos y el cumplimiento de la normativa aplicable. En este taller conocerás estas herramientas y te enseñaremos a utilizarlas.

Sesiones

1ª: 8 junio

2ª: 23 junio

TALLER 1: REGISTRO DE ACTIVIDADES DEL TRATAMIENTO

1.- Conceptos básicos

a) Dato de carácter personal. Es toda información relativa a una persona física, identificada o identificable.

- ❑ No son datos personales los datos de las personas jurídicas (Mi Empresa, S.A., un listado de fundaciones u organizaciones, etc.).
- ❑ Sí son datos personales los datos de personas de contacto dentro de empresas o Administraciones Públicas (un listado de contactos institucionales).
- ❑ No son datos personales las informaciones relativas a fallecidos.
- ❑ Aunque no tenga el nombre y el apellido, si puedo determinar a quién se refiere una información concreta por otros medios, se trata de un dato personal (es identificable).

Ejemplos de datos personales: los números de matrículas, los códigos de expedientes asociados a personas beneficiarias, los códigos de clientes, los números de empleado, los correos electrónicos, los DNIs, las fotos, las grabaciones de voz o vídeos.

b) Responsable del tratamiento y encargado del tratamiento.

El responsable del tratamiento es el "propietario" de los datos. Decide sobre la finalidad y medios del tratamiento. Actúa con autonomía e independencia.

El encargado del tratamiento es una entidad que accede a los datos para prestar un servicio al responsable. No es "propietario" de los datos y actúa siempre siguiendo las instrucciones del responsable.

RESPONSABLE	ENCARGADO
Decide sobre la finalidad y medios del tratamiento de forma autónoma e independiente.	Obedece las órdenes del responsable, aunque puede tomar decisiones operativas con cierta autonomía.
Tiene una relación directa (por ejemplo, un contrato) con los afectados y actúa frente a estos en nombre propio.	Cuando interactúa con los afectados, lo hace en nombre del responsable, no en nombre propio.
Es el "propietario" de los datos.	Es un prestador de servicios.
Tiene obligaciones directas de conservación de los datos o cumple una obligación legal al tratar los datos.	Sigue las instrucciones del responsable.
Atiende el ejercicio de derechos.	Solo atenderá el ejercicio de derechos si se lo indica el responsable.
Notifica brechas de seguridad a la AEPD.	Informa de las brechas de seguridad al responsable y colabora en su investigación.

Decide las bases de legitimación del tratamiento y redacta la política de privacidad o cláusula informativa.	No siempre aparece mencionado en la política de privacidad o cláusula informativa. Utiliza los textos redactados por el responsable.
TIENE PERSONALIDAD JURÍDICA PROPIA	**TIENE PERSONALIDAD JURÍDICA PROPIA**

c) Afectado o interesado. Es la persona física titular de los datos personales.

d) Tratamiento de datos. Consiste en cualquier operación que efectuemos sobre los datos personales, incluyendo el mero almacenamiento y la simple visualización.

2.- Marco legal básico

- 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 ("**RGPD**"). **Enlace a la norma**.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales ("**LOPDGDD**"). **Enlace a la norma**.

Puedes encontrar información de utilidad en la página web de la Agencia Española de Protección de datos, y en particular, en la sección "Cumple tus obligaciones". **Enlace a la sección**.

Y ADEMÁS…

Descarga de forma gratuita la Guía de la Agencia Española de Protección de Datos como complemento de este curso:

https://www.aepd.es/es/documento/guia-rgpd-para-responsables-de-tratamiento.pdf-0

3.- Descripción del modelo facilitado

Dispone de un documento Excel que contiene una plantilla para elaborar los registros de actividades del tratamiento ("**RATs**") de tu organización.

El RGPD dispone, en su artículo 30.1 que "*cada responsable y, en su caso, su representante, llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad*".

Esta obligación sustituye a la obligación de notificación de ficheros a la Agencia Española de Protección de Datos que recogía el anterior marco normativo.

El art. 30 del RGPD continúa indicando el contenido mínimo que deberá reflejarse en el RAT:

- El nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del Delegado de Protección de Datos.
- La identificación de las finalidades de cada tratamiento efectuado.
- Una descripción de las categorías de interesados y de los tipos de datos personales tratados.
- Las categorías de destinatarios a quienes se comunican los datos personales.
- Las transferencias de datos personales a un tercer país o a una organización internacional, incluyendo la identificación del país y las garantías adoptadas.
- Los plazos de conservación de las diferentes categorías de datos, cuando sea posible.
- Una descripción general de las medidas técnicas y organizativas de seguridad aplicadas, siempre que sea posible.

Igualmente, el art. 30 dispone que "*cada encargado y, en su caso, el representante del encargado llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable*". Se trata de un registro reducido o simplificado que deberá contener, al menos:

- El nombre y los datos de contacto del encargado y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del Delegado de Protección de Datos.
- Las categorías de tratamientos efectuados por cuenta de cada responsable.
- Las transferencias de datos personales a un tercer país u organización internacional, incluyendo la identificación del país y las garantías adoptadas.
- Una descripción general de las medidas técnicas y organizativas de seguridad aplicadas, cuando sea posible.

Nosotros nos centraremos en este primer taller en la elaboración de RATs de los que es responsable tu organización (es decir, en los tratamientos "propios").

No existe un formato único u oficial para elaborar un RAT. La plantilla que te facilitamos como modelo es un ejemplo. Podrías utilizar cualquier otro formato, siempre que incluya los contenidos del art. 30 del RGPD.

Las entidades podrán mantener el RAT en cualquier formato, incluido el electrónico, siempre que conste por escrito.

Tampoco existe una forma única de agrupar las actividades registradas: Una organización puede incluir en el mismo registro "gestión de trabajadores" y "gestión de procesos de selección", mientas que otra puede registrarlos de como RAT independientes.

La LOPDGDD, en su artículo 31, nos da una pista sobre cómo agrupar los tratamientos efectuados. Este artículo indica que el RAT "*podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, **según sus finalidades**, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento*".

Por tanto, una forma de agrupar operaciones de tratamiento es función de su finalidad.

¡RECUERDA!: Según dispone el artículo 30 del RGPD, todos los responsables y encargados están obligados a cooperar con la autoridad de control y poner a su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento.

3.- Trabajo previo al RAT

Antes de empezar a completar el RAT, debes conocer y entender todos los tratamientos que se realizan en tu organización.

Para ello, te recomendamos que completes dos tablas muy sencillas. La primera te ayudará a identificar quiénes tratan datos personales. En cada área o departamento, lo habitual es que exista uno o varios RATs. La segunda te servirá para entender el "ciclo de vida" de los datos personales, antes de completar la plantilla.

A) TABLA 1: Determina las áreas o departamentos que tratan datos personales

ÁREA/DEPARTAMENTO	FUNCIÓN	PERSONA RESPONSABLE
Legal	…	…
Gestión de Proyectos		
Voluntariado		
Relaciones institucionales		
….		

B) TABLA 2. Para cada área o departamento, completa la siguiente tabla:

PREGUNTA	RESPUESTA
¿A QUIÉN PERTENECEN LOS DATOS TRATADOS?	
¿QUÉ DATOS SE RECOGEN O GENERAN?	
¿PARA QUÉ SE USAN?	
¿CON QUIÉN SE COMPARTEN?	
¿DÓNDE SE GUARDAN?	
¿DURANTE CUÁNTO TIEMPO SE CONSERVAN?	
OBSERVACIONES	

RECUERDA:

- ❑ Tendremos una segunda sesión **NO GRABADA** para revisar el trabajo que habéis realizado y resolver vuestras dudas. No obstante, puedes **enviar cualquier consulta o duda a nuestro equipo a través del correo mododataprotection@gmail.com**

- ❑ No importa si no logras completar todos los RATs de la organización. Los podrás terminar después del curso. Al menos, debes finalizar dos RATs y listar los que te quedarían pendientes.

- ❑ **La segunda sesión del taller será el día 3 de febrero**

CONCEPTOS BÁSICOS

DATO DE CARÁCTER PERSONAL (ART. 4.1 RGPD)

*"Toda información sobre una **persona física identificada o identificable** («el afectado»); 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".*

EJEMPLO DE CATEGORÍAS DE DATOS PERSONALES OBJETO DE TRATAMIENTO

- **Datos identificativos:** nombre, apellidos, teléfono, e-mail, DNI/NIF de usuarios de servicios o del personal de EMT, nombre y apellido de firmantes y personas de contacto de contratos, convenios, acuerdos de colaboración, etc.
- **Datos de carácter académico y profesionales:** en la gestión de procedimientos selectivos, bolsas de empleo, recursos humanos.
- **Datos relativos a la utilización de sistemas y herramientas de trabajo:** nombre de usuarios de los medios tecnológicos y aplicaciones necesarias para el desempeño de tus funciones.
- **Datos económicos, financieros y de seguros**: cuentas bancarias para el abono de nóminas, información sobre seguros contratados para empleados, etc.

DATO DE CARÁCTER PERSNAL (ART. 4.1 RGPD)

Aquellos datos personales que revelen "*el* ***origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos*** *dirigidos a identificar de manera unívoca a una persona física,* ***datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales*** *de una persona física".*

- **Datos genéticos (art. 4.13 RGPD):** **"***datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona".*

- **Datos biométricos (art. 4.14 RGPD):** ***"****datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".*

- **Datos relativos a la salud (art. 4.15 RGPD):** **"***datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".*

EJEMPLO DE CATEGORÍAS DE DATOS PERSONALES ESPECIALMENTE PROTEGIDOS TRATADOS

Datos necesarios para la gestión de la relación laboral: grado de minusvalía (cuando existe y es relevante para el contrato de trabajo), bajas por enfermedad y accidente de trabajo, información facilitada voluntariamente por el empleado para justificar ausencias o permisos, etc. **Datos incluidos en partes de accidentes o reclamaciones**.

TRATAMIENTO DE LOS DATOS (ART. 4.2 RGPD)

"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".

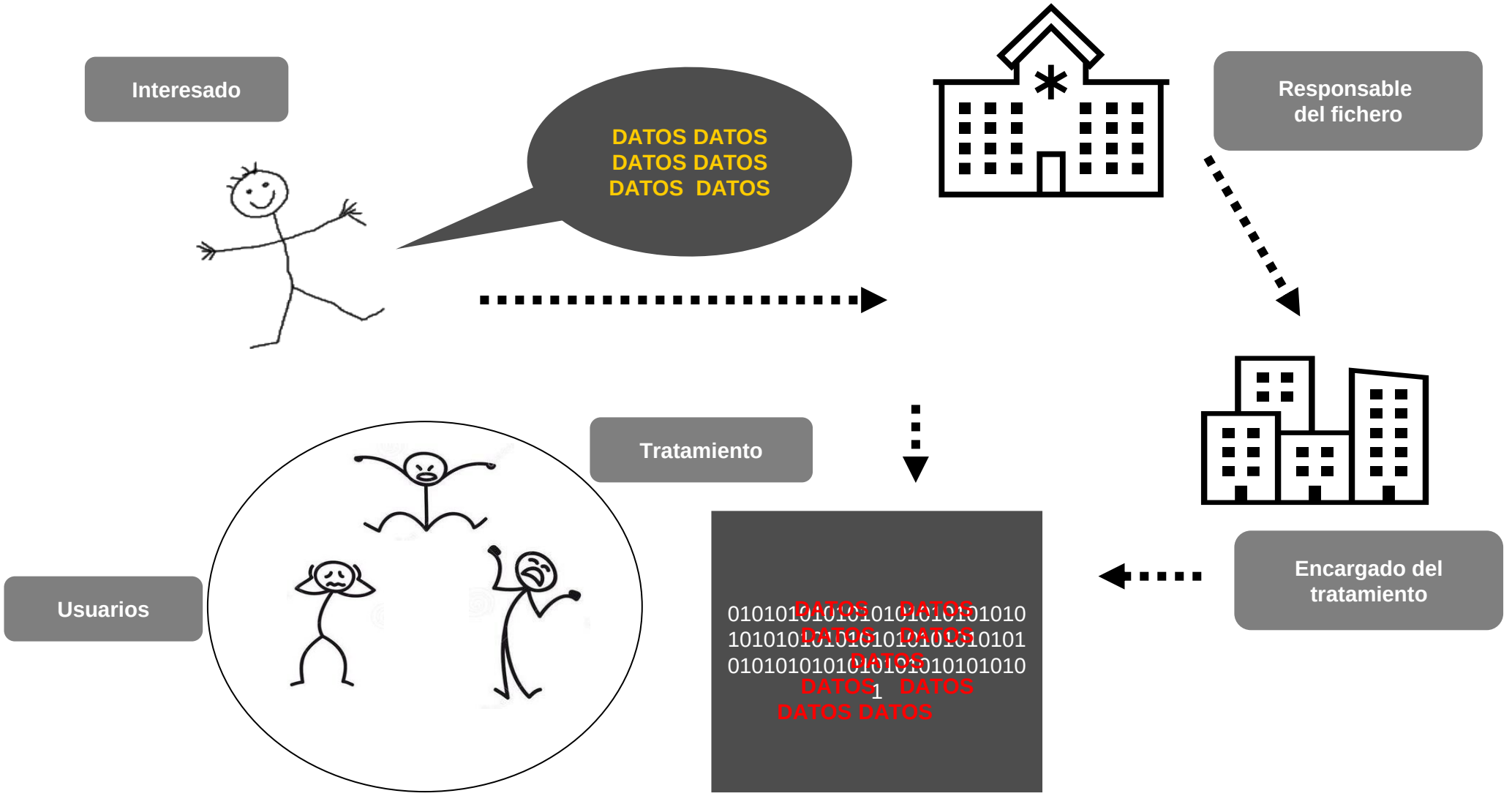
RESPONSABLE DE TRATAMIENTO (ART. 4.7 RGPD)

"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".
Ejemplo: Una ONG es responsable del tratamiento de gestión de personal, gestión de actividades voluntarias, formación de personal, etc.

ENCARGADO DEL TRATAMIENTO

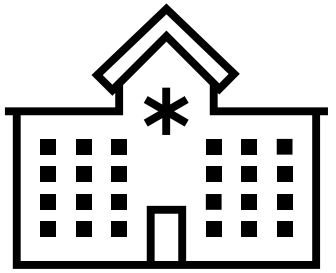
"La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".
El encargado del tratamiento es, normalmente, un prestador de servicios que no tiene capacidad de decisión sobre el tratamiento (no lo puede usar para fines propios).
Ejemplo: Gestoría encargada de la llevanza de las nóminas.

CONCEPTOS BÁSICOS



CICLO DE VIDA DE LOS DATOS

1. Recogida de los datos



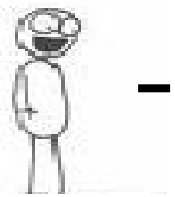
Información Y base de legitimación

2. Almacenamiento de los datos

- Registro de actividades de tratamiento
- Medidas de Seguridad
- Contratos E. T.
- Calidad de datos

3. Acceso y Uso de los datos

- Respetar las medidas de seguridad en el acceso a los datos
- Guardar secreto



DATOS DATOS DATOS DATOS DATOS

¿QUÉ ES UN RAT?

El **registro de actividades del tratamiento o RAT** recoge el detalle de las actividades u operaciones de tratamiento que efectúa una entidad en el desarrollo de sus actividades. Con el RGPD, desaparece la obligación de notificar la inscripción de ficheros en el registro de la Agencia Española de Protección de Datos.

¿Qué es una actividad de tratamiento? No hay una definición legal. En un conjunto de operaciones de tratamiento que algo tienen en común que nos permite agruparlas: la finalidad (los objetivos os del tratamiento), la tipología de datos o los titulares de estos.

RECURSOS HUMANOS (TRABAJADORES)	***VOLUNTARIOS***	***PROYECTOS***	***CONTABILIDAD Y FINANZAS***

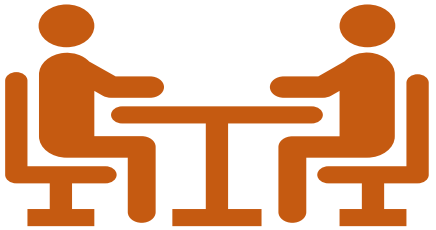
El art. 30.1 del RGPD señala el contenido mínimo del RAT:

- ❑ **Nombre y datos de contacto del responsable y del delegado de protección de datos delegado.**
- ❑ **Fines del tratamiento de los datos personales que trata EMT.**
- ❑ **Descripción categorías interesados y categorías datos personales.**
- ❑ **Categorías de destinatarios.**
- ❑ **Transferencias internacionales de datos a terceros países.**
- ❑ **Plazos de supresión de los datos.**

¿Qué información necesito conocer sobre mi ONG antes de empezar a completar el RAT?

Debemos tener claro los tratamientos que se efectúan en la organización. Normalmente, partimos de un organigrama de la organización y realizamos entrevistas con los responsables de cada área, departamento o dirección.

- **¿Qué áreas, departamentos o direcciones tratan datos personales en tu ONG?**
  - RR HH
  - Financiero / Contabilidad / Facturación / Compras
  - Legal
  - Gestión de ProyectosObtención de fondos / Imagen corporativa / Márketing
  - Tecnología / Informática
  - (…..)



- **¿Qué tengo que saber de cada área?**
  - ¿Qué datos trato?´
  - ¿De quién son los datos personales?
  - ¿Cómo los recojo y dónde los almaceno?
  - ¿Para qué los uso?
  - ¿Con quién los comparto?

MANOS A LA OBRA…..

¿De quién son los datos?
Voluntarios, empleados, beneficiarios, cargos en instituciones, donantes…

¿Con quién los comparto?
Proveedores, Administración Pública, ……

¿Qué datos se recogen?
Fotos, nombre y apellidos, teléfonos, datos de contacto, cuanta bancaria…..

¿Qué hago con los datos?
Gestión de proyectos, recogida de fondos, gestión de contratos, pago de nóminas, publicidad de actividades……

¿Dónde los guardo?

¿Qué me habilita a tratarlos?
Una ley, un contrato, el consentimiento….

¿Durante cuánto tiempo los necesito?

MANOS A LA OBRA…..

RR HH

FASE I: Recogida de datos. Envío de CV y prueba de selección.
Tipo de datos: Nombre, apellidos, experiencia profesional, datos de contacto, CV.
Categoría de afectado: Empleados

FASE II: Uso de los datos. Se utilizan para gestionar la relación laboral: contrato, nóminas, vacaciones, bajas, etc.
Se almacenan en un archivado en papel y en un programa de nóminas

Trabajador

FASE III: Destinatarios de los datos. Una gestoría presta servicios como encargado del tratamiento. Se ceden a la TGSS, a la Mutua y al SPA.

FASE IV: Fin del tratamiento. Cuando el trabajador se va a otro empleo, se archiva su expediente en papel y se bloquean sus datos en el programa durante, al menos, 5 años. Se comunica su baja a la TSGG, Mutua, SPA y gestoría

TALLER 2: CÓMO REDACTAR UNA POLÍTICA O CLÁUSULA INFORMATIVA DE PRIVACIDAD

1.- Cuestiones básicas

a) El deber de informar

- ❑ Regla general: antes de tratar datos personales, obligación de informar
  - ¿De qué tenemos que informar?
  - ¿Cómo podemos informar?
  - ¿Cuándo tenemos que informar?
- ❑ Ejemplos
  - Empleados
  - Socios / miembros de la fundación
  - Beneficiarios
  - Videovigilancia
- ❑ Artículos 13 y 14 RGPD
  - Artículo 13 RGPD: cuando los datos se han obtenido del interesado
  - Artículo 14 RGPD: cuando los datos no se han obtenido del interesado
- ❑ ¿Quién debe informar? La obligación recae sobre el responsable del tratamiento
- ❑ Libertad de forma (en papel, verbal), aunque se aconseja guardar prueba de que se ha cumplido con el deber de información

b) El principio de transparencia

- ❑ Además de facilitar la información, esta debe ser presentada de forma transparente
- ❑ Artículo 12.1 RGPD: información concisa, transparente, inteligible y de fácil acceso, lenguaje claro y sencillo (en especial, niños), por escrito o por otros medios
- ❑ "concisa, transparente, inteligible y de fácil acceso"
- ❑ "lenguaje claro y sencillo"

2.- Marco legal básico

- Reglamento General de Protección de Datos: **https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32016R0679**

- Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales: **https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673**

- Directrices sobre la transparencia en virtud del RGPD, adoptadas el 29 de noviembre de 2017 por el Grupo de Trabajo del Artículo 29: **https://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/wp260rev01_es-transparencia.pdf**

- Guía para el cumplimiento del deber de informar de la Agencia Española de Protección de Datos: **https://www.aepd.es/sites/default/files/2019-09/guia-modelo-clausula-informativa.pdf**

3.- Instrucciones para completar los modelos

Junto con la presentación de la clase del jueves 10 de febrero se han facilitado cuatro modelos de cláusulas informativas:

- ❑ Modelo política de privacidad
- ❑ Modelos primera capa informativa
- ❑ Modelo cláusula de los firmantes
- ❑ Modelo cláusula informativa trabajadores

De cara a la próxima sesión, os pedimos que completéis el documento "Modelo política de privacidad" con los tratamientos que lleváis a cabo en el marco de vuestra fundación / asociación. Podéis centrarlo en unos tratamientos en concreto (p.e., datos personales de los socios de la fundación) o preparar un modelo más exhaustivo que cubra todos los tratamientos. Recordad que, además de incluir toda la información necesaria, es preciso hacerlo de forma clara y entendible, para así cumplir con el principio de transparencia.
Además de corregir el trabajo que hayáis realizado, podemos aprovechar la próxima sesión para comentar el resto de documentos ("Modelo de cláusula de los firmantes", "Modelo de Primera Capa" y "Modelo cláusula empleados").

RECUERDA:

- ❑ Tendremos una segunda sesión **NO GRABADA** para revisar el trabajo que habéis realizado y resolver vuestras dudas. No obstante, puedes **enviar cualquier consulta o duda a nuestro equipo a través del correo mododataprotection@gmail.com**

- ❑ No importa si no logras completar todos los modelos. Los podrás terminar después del curso.

- ❑ **La segunda sesión del taller será el día 24 de febrero**

El deber de informar: general

- ❑ Regla general: antes de tratar datos personales, obligación de informar
  - ¿**De qué** tenemos que informar?
  - ¿**Cómo** podemos informar?
  - ¿**Cuándo** tenemos que informar?
- ❑ Ejemplos
  - Empleados
  - Socios / miembros de la fundación
  - Beneficiarios
  - Videovigilancia
- ❑ Artículos 13 y 14 RGPD
  - Artículo 13 RGPD: cuando los datos se han obtenido del interesado
  - Artículo 14 RGPD: cuando los datos **no** se han obtenido del interesado
- ❑ ¿Quién debe informar? La obligación recae sobre el **responsable del tratamiento**
- ❑ Libertad de forma (en papel, verbal), aunque se aconseja guardar prueba de que se ha cumplido con el deber de información

El deber de informar: ¿de qué tengo que informar? (1)

Identidad y datos de contacto del responsable

- Ejemplo: *Servicios Integrales Sipa, S.A. con CIF B-233456 y dirección en calle Alegría 4, 08050 Barcelona, teléfono 931234567, y dirección de correo electrónico info@sisipa.com*

❑ Datos de contacto del delegado de protección de datos (si se ha designado)

- Ejemplo: *Podrás contactar con nuestro delegado de protección de datos en la siguiente dirección: delegadoRGPD@sisipa.com*

❑ Finalidad/es del tratamiento y su/s base/s jurídica/s

- Ejemplo: *Tratamos los datos de carácter personal que nos has facilitado para poder prestarte los servicios solicitados. La base jurídica del tratamiento es la ejecución de contrato suscrito con nosotros (art. 6.1b) RGPD)*

✓ Si la base jurídica es el interés legítimo: indicar cuál es ese interés legítimo

✓ Si la base jurídica es la ejecución de un contrato: indicar cuál es ese contrato

✓ Si la base jurídica es el cumplimiento de una obligación legal: indicar la ley

Los destinatarios o categorías de destinatarios de los datos personales (si se quieren ceder los datos a un tercero)

- Ejemplo: *Tus datos de carácter personal se comunicarán a empresas del sector de la educación que habitualmente colaboran con nosotros ayudándonos en la prestación de los servicios solicitados*

❑ La intención del responsable de llevar a cabo transferencias internacionales de datos (caso en que los datos salen fuera del EEE)

- Ejemplo: *Tus datos de carácter personal serán transferidos a Suiza, país respecto del que la Comisión Europea ha adoptado una decisión de adecuación*

❑ Plazo de conservación de los datos o criterios utilizados para determinar el plazo

- Ejemplo: *Conservaremos tus datos durante la vigencia de la relación contractual que nos une y, con posterioridad, durante el periodo tiempo en el que estemos obligados por ley a conservar dichos datos. Transcurrido dicho periodo, los mantendremos bloqueados durante el periodo de tiempo legalmente establecido en el que puedan derivarse responsabilidades entre las partes*

El deber de informar: ¿de qué tengo que informar? (2)

Los derechos del interesado. Ejemplo: *Puedes ejercer tus derechos de acceso, rectificación, supresión y portabilidad de tus datos, de limitación y oposición a su tratamiento, así como a no ser objeto de decisiones individuales automatizadas y a retirar el consentimiento que nos hayas podido prestar enviando un correo electrónico a protecciondedatos@sisipa.com*

- ✓ Si el tratamiento se basa en el consentimiento: el derecho a retirar el consentimiento
- ❑ El derecho a presentar una reclamación ante una autoridad de control. Ejemplo: *Puedes presentar una reclamación ante la Agencia Española de Protección de Datos (www.aepd.es), especialmente cuando no hayas obtenido satisfacción en el ejercicio de tus derechos*
- ❑ La existencia de decisiones automatizadas (elaboración de perfiles)
  - Decisiones que producen efectos sobre el individuo y en las que no interviene un elemento humano en la toma de la decisión
  - En estos casos, dar información significativa sobre (i) la lógica aplicada y (ii) la importancia y las consecuencias previstas de dicho tratamiento para el interesado
- ❑ Las categorías de datos personales de que se trate. Ejemplo: *Los datos de carácter personal que nos han sido proporcionados consisten en los datos contenidos en tu currículum*
- ❑ Fuente de la que proceden los datos personales. Ejemplo: *Tus datos de carácter personal han sido proporcionados por/proceden de Fundación Ilusión*
- ❑ Dos opciones:
  - En una sola vez: **https://www.msf.es/politica-de-privacidad**
  - Por capas (artículo 11 LOPDyGDD):
    - Primera capa:
      - Identidad del responsable
      - Finalidad/es del tratamiento
      - Posibilidad de ejercer derechos
      - Elaboración de perfiles, en su caso
      - Categorías de datos y fuentes de las que proceden los datos (artículo 14 RGPD)
      - Dirección electrónica u otro medio en el que acceder al resto de información
    - Segunda capa: resto de información

El deber de informar: ¿cómo puedo informar? (1)

- Ejemplo de primera capa:

  Fundación Iguana, en calidad de responsable del tratamiento, tratará los datos personales facilitados para gestionar la prestación de los servicios solicitados.

  Podrás ejercer los derechos de acceso, rectificación, supresión, oposición, limitación, así como tu derecho a la portabilidad de los datos, dirigiendo tu petición a la siguiente dirección de correo electrónico: datos@figuana.org.

  Encontrarás más información sobre el tratamiento de tus datos de carácter personal en el siguiente enlace [enlace a la segunda capa]

- Segunda capa:
  - Debe ser completa
  - Lenguaje claro, conciso y comprensible: “preguntas y respuestas”, concisión y precisión y evitar el abuso de la “jerga” legal
  - Responsable: dirección postal y, si se dispone de ella, dirección electrónica
  - Finalidad: no incluir finalidades demasiado genéricas que puedan conducir a tratamientos ulteriores que excedan de las expectativas razonables del interesado
  - Si la base legal es la ejecución del contrato: identificar el contrato; si es el cumplimiento de una obligación legal: identificar la norma; si es el interés legítimo: identificar los intereses
  - Hacer constar si el interesado está obligado a facilitar los datos y las consecuencias de no hacerlo
  - Conveniente informar sobre la existencia de encargados del tratamiento
  - Transferencias internacionales: mecanismo de cobertura

El deber de informar: ¿cuándo tengo que informar? (1)

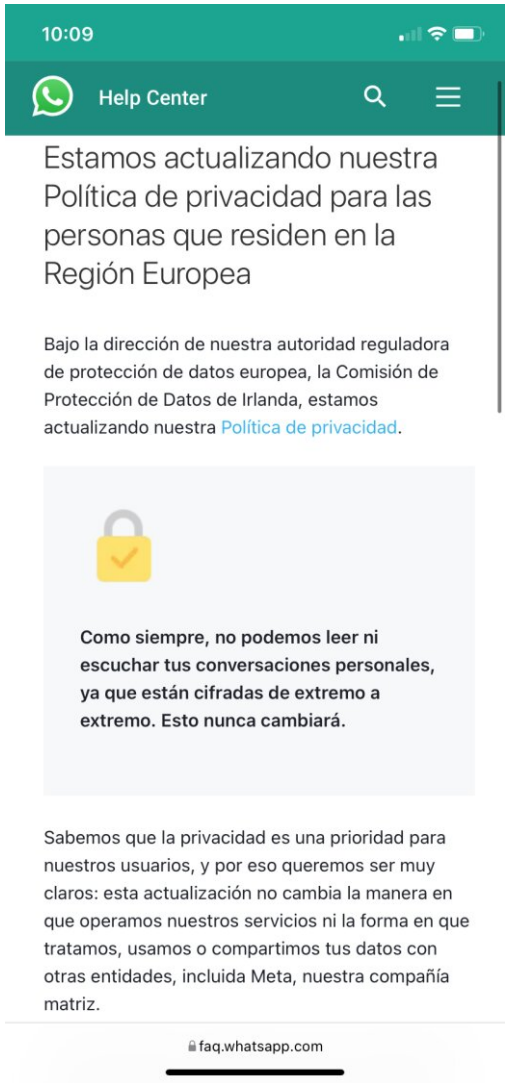
Dos supuestos

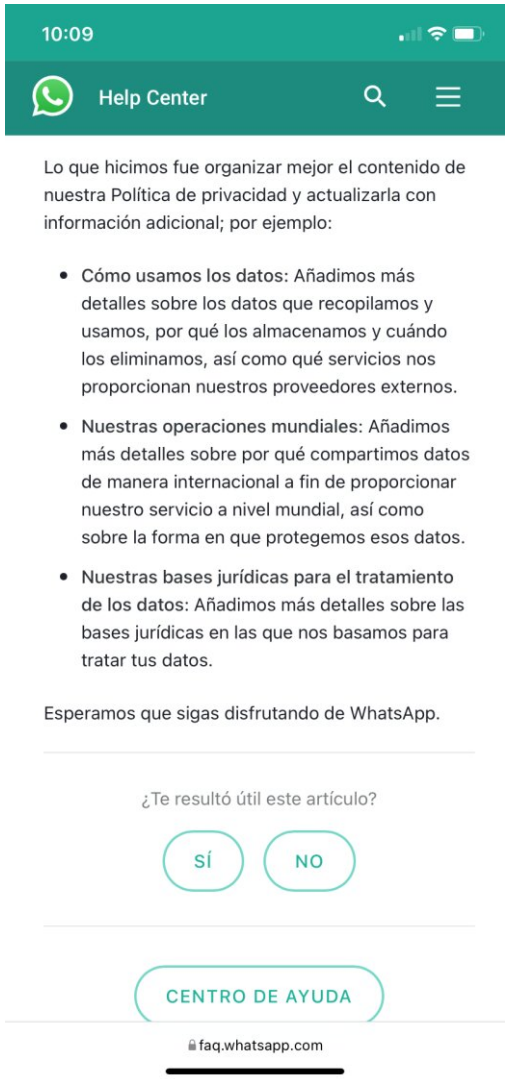
- Cuando el responsable ha obtenido los datos del interesado (artículo 13 RGPD): con carácter previo al tratamiento ("*en el momento en que estos se obtengan*")
- Cuando el responsable no haya obtenido los datos del interesado, sino de un tercero (artículo 14 RGPD):
  - Como es lógico, no se puede informar antes del tratamiento
  - En un máximo de **1 mes** desde la obtención de los datos personales, excepto:
    a) Si los datos personales han de utilizarse para una comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado
    b) Si se quieren comunicar a otro destinatario, a más tardar en el momento en que los datos sean comunicados por primera vez

- ❑ El deber de información se aplica a lo largo de todo el ciclo de vida del tratamiento
- ❑ ¿Debo informar de los cambios en la política / cláusula de privacidad?

  SÍ
- ❑ ¿En cualquier caso?
  - Cambio en el fin del tratamiento
  - Cambio en la identidad del responsable
  - Cambio en la forma en que pueden ejercitarse los derechos
  - Errores tipográficos, gramaticales o de estilo
- ❑ ¿Cómo y cuándo comunicamos el cambio?
  - Comunicación dedicada específicamente a ello
  - Si el cambio es relevante, con suficiente antelación antes de que se produzca
  - Que el cambio no pase inadvertido
  - Valorar "refrescar" la información de forma periódica

El deber de informar: ¿cuándo tengo que informar? (2)





El deber de informar: ¿cuándo no tengo obligación de informar?

- ❑ Regla general: informar antes del tratamiento o en los plazos indicados por el artículo 14 RGPD
- ❑ Excepciones al deber de informar:
  - Si el interesado ya dispone de la información (artículos 13 y 14 RGPD)
  - Por imperativo legal (artículo 14 RGPD)
    - ✓ Ley de Prevención del Blanqueo de Capitales:

      "*3. En virtud de lo dispuesto en el artículo 24.1, y en relación con las obligaciones a las que se refiere el apartado anterior, no será de aplicación al tratamiento de datos la obligación de información prevista en el artículo 5 de la Ley Orgánica 15/1999*"
  - Imposible o esfuerzo desproporcionado, o si pudiera imposibilitar u obstaculizar gravemente el logro de los objetivos del tratamiento (interpretación restrictiva) (artículo 14 RGPD)

Transparencia: general

- ❑ Además de facilitar la información, esta debe ser presentada de forma **transparente**
- ❑ Artículo 12.1 RGPD: información concisa, transparente, inteligible y de fácil acceso, lenguaje claro y sencillo (en especial, niños), por escrito o por otros medios

Transparencia: "concisa, transparente, inteligible y de fácil acceso"

Fatiga informativa

- ❑ Diferenciar la información relativa a la privacidad de la información no relacionada con la privacidad
- ❑ Comprensible al integrante medio de la audiencia objetivo
  - Fácil acceso: el interesado no debe tener que buscar la información
  - Sitio web: en cada una de las páginas web dentro del sitio web debería aparecer, de manera claramente visible, un enlace directo a la política de privacidad
  - Aplicaciones: la información debería estar disponible en la tienda en línea antes de la descarga
- ❑ ¿Cuántos "clics" se recomiendan antes de llegar a la información?

Transparencia: "lenguaje claro y sencillo"

- ❑ Facilitarse de la forma más simple posible
- ❑ Evitar oraciones y estructuras lingüísticas complejas
- ❑ Finalidades y base jurídica especialmente claros
- ❑ Evitar el uso de "puede", "podría", "algunos", "frecuentemente" y "posible"
- ❑ Evitar lenguaje o terminología excesivamente legal o técnica
- ❑ Las traducciones deben ser fieles

TALLER 3: EJERCICIO DE DERECHOS DE LOS AFECTADOS

1.- Conceptos básicos

a) Dato de carácter personal.

Es toda información relativa a una persona física, identificada o identificable.

- ❑ No son datos personales los datos de las personas jurídicas (Mi Empresa, S.A., un listado de fundaciones u organizaciones, etc.).
- ❑ Sí son datos personales los datos de personas de contacto dentro de empresas o Administraciones Públicas (un listado de contactos institucionales).
- ❑ Aunque no tenga el nombre y el apellido, si puedo determinar a quién se refiere una información concreta por otros medios, se trata de un dato personal (es identificable).

b) Responsable del tratamiento y encargado del tratamiento.

El responsable del tratamiento es el "propietario" de los datos. Decide sobre la finalidad y medios del tratamiento. Actúa con autonomía e independencia.

El encargado del tratamiento es una entidad que accede a los datos para prestar un servicio al responsable. No es "propietario" de los datos y actúa siempre siguiendo las instrucciones del responsable.

c) Afectado o interesado.

Es la persona física titular de los datos personales.

d) Tratamiento de datos.

Consiste en cualquier operación que efectuemos sobre los datos personales, incluyendo el mero almacenamiento y la simple visualización.

2.- Características de los derechos reconocidos por la normativa de protección de datos

- ❑ Su ejercicio es gratuito.
- ❑ Si las solicitudes son manifiestamente infundadas o excesivas (p.ej., carácter repetitivo) el responsable podrá (i) cobrar un canon proporcional a los costes administrativos soportados, (ii) negarse a actuar.
- ❑ Las solicitudes deben responderse en el plazo de un mes, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más.
- ❑ El responsable está obligado a informarte sobre los medios para ejercitar estos derechos. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio.
- ❑ Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.
- ❑ Si el responsable no da curso a la solicitud, informará, a más tardar en un mes, de las razones de su no actuación y de la posibilidad de reclamar ante una Autoridad de Control.
- ❑ Se pueden ejercer los derechos directamente o por medio de tu representante legal o voluntario.

- ❑ Cabe la posibilidad de que el encargado sea quien atienda la solicitud por cuenta del responsable si ambos lo han establecido en el contrato o acto jurídico que les vincule.

3- Marco legal básico y documentos de interés

- 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 ("**RGPD**"). **Enlace a la norma**.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales ("**LOPDGDD**"). **Enlace a la norma**.

- Documentos de interés:

  Infografía de la AEPD "Cuáles son tus derechos": https://www.aepd.es/es/documento/cuales-son-tus-derechos-de-proteccion-de-datos.pdf

  Infografía de la AEPD "Derechos de los ciudadanos": https://www.aepd.es/es/documento/infografia-rgpd-derechos-ciudadanos-aepd.pdf

4.- Descripción del caso práctico

El caso práctico consiste en la elaboración de un protocolo de actuación o política interna que nos permita atender de forma ordenada y dentro de plazo las solicitudes de los afectados. Este documento deberá contener:

(i) Una explicación de cuáles son los derechos que una persona puede ejercer de acuerdo con el RGPD.

(ii) Una descripción clara de cómo se debe actuar si se recibe una petición por correo electrónico, teléfono o carta: a quién remitir la petición internamente, en qué plazo dar respuesta, por qué medio contactar al afectado; qué hacer si no figura en nuestra base de datos, etc.

(iii) La designación de una persona responsable de gestionar el proceso.

(iv) Un modelo de respuesta para los derechos que consideramos más frecuentes: acceso a datos, supresión y oposición al envío de comunicaciones comerciales.

[*Para elaborar esta política, el alumno deberá seguir el modelo que se facilita en formato Word*].

RECUERDA:

- ❑ Tendremos una segunda sesión **NO GRABADA** para revisar el trabajo que habéis realizado y resolver vuestras dudas. No obstante, puedes **enviar cualquier consulta o duda a nuestro equipo a través del correo mododataprotection@gmail.com**

- ❑ **La segunda sesión del taller será el día 17 de marzo.**

CONCEPTOS BÁSICOS

RESPONSABLE DE TRATAMIENTO (ART. 4.7 RGPD)

"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". **Ejemplo: Una ONG es responsable del tratamiento de gestión de personal, gestión de actividades voluntarias, formación de personal, etc.**

ENCARGADO DEL TRATAMIENTO (ART. 4.8 RGPD)

"La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento". El encargado del tratamiento es, normalmente, un prestador de servicios que no tiene capacidad de decisión sobre el tratamiento (no lo puede usar para fines propios).

TRANSPERENCIA DE LA INFORMACIÓN, COMUNICACIÓN Y MODALIDADES DE EJERCICIO DE LOS DERECHOS DEL INTERESADO (ART. 12 RGPD)

El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes.

LOS DERECHOS CONTEMPLADOS EN LOS ART. 15 A 22 RGPD SON:

1º. Derecho de Acceso
2º. Derecho de Rectificación
3º. Derecho de Oposición
4º. Derecho de Supresión
5º. Derecho a la Limitación del Tratamiento
6º. Derecho a la Portabilidad
7º. Derecho a no ser Objeto de Decisiones Automatizadas

CARACTERISTICAS DE LOS DERECHOS DE PROTECCIÓN DE DATOS

Estos derechos **se caracterizan por lo siguiente**:

- Su ejercicio es **gratuito.**
- Si las solicitudes son **manifiestamente infundadas o excesivas** (p.ej., carácter repetitivo) el responsable podrá (i) cobrar un **canon** proporcional a los costes administrativos soportados, (ii) **negarse** a actuar.
- Las solicitudes **deben responderse en el plazo de un mes**, aunque, si se tiene en cuenta la complejidad y número de solicitudes, se puede prorrogar el plazo otros dos meses más.
- El responsable está obligado a **informarte sobre los medios para ejercitar estos derechos**. Estos medios deben ser accesibles y no se puede denegar este derecho por el solo motivo de que optes por otro medio.
- Si la solicitud se presenta por **medios electrónicos**, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.
- Si **el responsable no da curso a la solicitud, informará y a más tardar en un mes**, de las razones de su no actuación y la posibilidad de reclamar ante una Autoridad de Control.
- Puedes **ejercer los derechos directamente o por medio de tu representante legal o voluntario.**
- Cabe **la posibilidad de que el encargado sea quien atienda tu solicitud por cuenta del responsable** si ambos lo han establecido en el contrato o acto jurídico que les vincule.

DERECHO DE ACCESO (ART. 15 RGPD)

El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, ***derecho de acceso a los datos personales*** *y a la siguiente información:*

- ❑ **Los fines del tratamiento.**
- ❑ **Las categorías de datos personales de que se trate.**
- ❑ **Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales.**
- ❑ **De ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.**
- ❑ **La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;**
- ❑ **El derecho a presentar una reclamación ante una autoridad de control.**
- ❑ **Cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen.**
- ❑ **La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.**

DERECHO DE RECTIFICACIÓN (ART. 16 RGPD)

El interesado tendrá derecho a obtener, sin dilación indebida del responsable del tratamiento, la rectificación de los datos personales inexactos que le conciernan.

Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional. En la solicitud, el interesado debe indicar los datos a corregir o, en su caso, completar y precisar los términos de dicha corrección.

Cuando resulte necesario, el interesado debe acompañar la documentación justificativa de la inexactitud o carácter incompleto de los datos.

DERECHO DE OPOSICIÓN (ART. 21 RGPD)

El interesado tendrá derecho a **oponerse en cualquier momento** a que datos personales que le conciernan (incluida la elaboración de perfiles) sean objeto de un tratamiento basado en los siguientes supuestos:

- Tratamientos necesarios para el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable.
- Tratamientos necesarios para la satisfacción de intereses legítimos del responsable o de un tercero.

El responsable del tratamiento dejará de tratar los datos personales, **salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades** del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

Cuando el tratamiento de datos tenga como finalidad el desarrollo de actividades de **marketing directo**, los interesados tendrán derecho a oponerse a dicho tratamiento en cualquier momento, incluida la elaboración de perfiles.

A más tardar en el momento de la primera comunicación con el interesado, el derecho de oposición será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos (artículo 89.1), el interesado tendrá derecho, a oponerse al tratamiento de datos personales que le conciernan, **salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.**

DERECHO DE SUPRESIÓN "DERECHO AL OLVIDO" (ART. 17 RGPD)

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

- ❑ los datos personales ya **no sean necesarios** en relación con los fines para los que fueron recogidos o tratados de otro modo.
- ❑ el **interesado retire el consentimiento** en que se basa el tratamiento de conformidad, y este no se base en otro fundamento jurídico.
- ❑ el **interesado se oponga al tratamiento** y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2.
- ❑ los datos personales hayan sido **tratados ilícitamente.**
- ❑ los datos personales **deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros** que se aplique al responsable del tratamiento.
- ❑ los datos personales se hayan **obtenido en relación con la oferta de servicios de la sociedad de la información.**

No se suprimirá la información cuando el tratamiento sea necesario:

- ❑ para ejercer el **derecho a la libertad de expresión e información.**
- ❑ para el **cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros** que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable.
- ❑ por razones de **interés público** en el ámbito de la **salud pública**.
- ❑ con **fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos**, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o
- ❑ para la **formulación, el ejercicio o la defensa de reclamaciones.**

DERECHO DE LIMITACIÓN DEL TRATAMIENTO (ART. 18 RGPD)

El interesado tendrá **derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos** cuando se cumpla alguna de las condiciones siguientes:

- **El interesado 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 el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.**
- **El responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.**
- **El interesado se haya opuesto al tratamiento, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.**

Cuando el tratamiento de datos personales se haya limitado, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

DERECHO A LA PORTABILIDAD (ART. 20 RGPD)

Qué comprende →

Derecho a recibir los datos personales, que el interesado haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a **transmitirlos a otro responsable del tratamiento** sin que lo impida el responsable al que se los hubiera facilitado, cuando:

- El tratamiento esté basado en el consentimiento (consentimiento explícito en caso de datos especialmente protegidos).
- el tratamiento se efectúe por medios automatizados.

Cómo hacer efectivo el derecho →

Al ejercer su derecho a la portabilidad de los datos, el interesado tendrá **derecho a que los datos personales se transmitan directamente de responsable a responsable** cuando sea técnicamente posible.

No afecta a otros derechos →

- El ejercicio del derecho **se entenderá sin perjuicio del derecho de acceso. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos** conferidos al responsable del tratamiento.

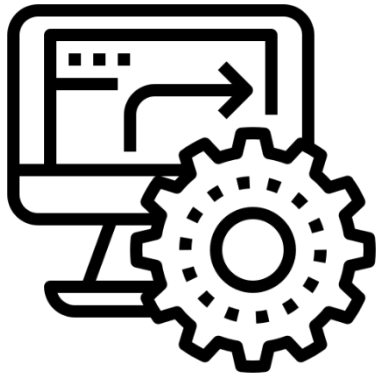
- El derecho a la portabilidad de los datos **no afectará negativamente a los derechos y libertades de otros.**

DECISIONES INDIVIDUALES AUTOMATIZADAS, INCLUIDA ELABORACIÓN DE PERFILES (ART. 22 RGPD)

Todo interesado tendrá **derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado**, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Excepto si la decisión:

- ❑ Es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
- ❑ Está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o
- ❑ Se basa en el consentimiento explícito del interesado.



CUESTIONES PRÁCTICAS

¿Si recibo una petición de ejercicio de derechos por un cauce que NO es el establecido en mi política de privacidad, ¿puedo desestimarla por tal motivo?

No. La AEPD determinó en el TD/0027/2020 que la petición deberá remitirse al Delegado de Protección de Datos o al departamento/persona responsable de la atención de los derechos del afectado para su tramitación. Por ello, es importante disponer de un protocolo interno que determine los pasos a seguir y formar al personal para que sepa cómo actuar cuando alguien ejerce sus derechos (por ejemplo, en el transcurso de una comunicación habitual de atención al cliente).

¿Se debe facilitar el acceso a las grabaciones de voz de los clientes?

Sí, puesto que la voz es un dato de carácter personal. No obstante, debemos tener en cuenta que en ocasiones el derecho no puede ser atendido porque (i) no se dispone de la grabación (es decir, ha sido borrada) o (ii) no se puede localizar con la información que aporta el afectado en su escrito.

En el segundo caso, podemos responderle pidiéndole datos adicionales que nos ayuden en nuestra búsqueda. Para evitar afectar derechos de terceros (la voz de otra persona), se admite la entrega de una transcripción de la conversación, así lo explica el procedimiento de la AEPD TD/00098/2020.

¿Debo responder a todas las peticiones de ejercicio de derechos, incluso a aquellas que se denieguen por ser manifiestamente infundadas?

Sí. Aunque la respuesta a la solicitud sea la denegación del derecho, se debe enviar una respuesta formal al afectado dentro del plazo establecido. En el procedimiento TD/00279/2020, la AEPD aclara:

"*En el supuesto aquí analizado, la parte reclamante ejercitó su derecho de supresión de sus datos personales incluidos en los ficheros de Solvencia Patrimonial y Cirbe, y conforme a las normas antes señaladas, su solicitud no obtuvo la respuesta legalmente exigible, dado que no se acredita la respuesta a dicha petición.*

Las normas antes citadas no permiten que pueda obviarse la solicitud como si no se hubiera planteado, dejándola sin la respuesta que obligatoriamente deberán emitir los responsables, aún en el supuesto de que no existan datos del interesado en los ficheros de la entidad o incluso en aquellos supuestos en los que no reuniera los requisitos previstos, en cuyo caso el destinatario de esta viene igualmente obligado a requerir la subsanación de las deficiencias observadas o en su caso, denegar la solicitud motivadamente indicando las causas por las que no procede considerar la supresión de sus datos.

Por tanto, la solicitud de supresión de los datos personales que se formule obliga al responsable que se trate a dar respuesta expresa, en todo caso, empleando para ello cualquier medio que justifique la recepción de la contestación".

CUESTIONES PRÁCTICAS

¿Tengo que probar que he atendido una solicitud ARCO Plus? ¿Por qué medio debo responder al afectado?

En el procedimiento TD/00220/2020, la empresa reclamada alegó que respondió a la petición del afectado, pero que no puede probarlo debido a un problema informático:

"La reclamada a pesar de que señala que, atendió el derecho, pero que no puede acreditarlo por un error informático, cabe señalar que, durante la tramitación de este procedimiento tuvo la oportunidad de subsanar dicha anomalía, como así está previsto en el RGPD, particularmente las que responden a los principios de transparencia y responsabilidad proactiva, para que se informe y se acredite ante esta Agencia de las acciones llevadas a cabo para atender la reclamación planteada".

La AEPD estimó la petición del afectado por motivos formales e insta al responsable a enviarle certificación por la que se atienda el derecho de supresión o se deniegue motivadamente. De esta resolución podemos sacar dos conclusiones básicas:

- **La primera**: nunca es tarde para atender la solicitud de un afectado y ganar puntos con la AEPD demostrando nuestra buena disposición.
- **La segunda**: el principio de responsabilidad proactiva obliga al responsable del tratamiento no solo a cumplir, sino a estar en condiciones de demostrar que cumple. Por este motivo, la generación de evidencias (registros en Excel, logs informáticos, políticas debidamente aprobadas, etc.) adquiere una gran importancia con el Reglamento General de Protección de Datos.

Ahora bien, ¿significa esto que debemos responder siempre a los afectados por burofax o correo certificado con el consiguiente gasto? No necesariamente. Dependiendo del contexto, se puede responder, por ejemplo, por correo electrónico. Entra dentro de lo razonable esperar que, si la AEPD admite como prueba del ejercicio del derecho un correo electrónico enviado por el afectado, también va a admitir como prueba de su atención un correo electrónico enviado por el responsable del tratamiento. Es más, en muchos casos, no se dispone de dirección física, solo de un email. Enviar una contestación por burofax implicaría recoger datos adicionales.

Una buena práctica puede ser responder las peticiones por el mismo medio por el que llegan, salvo que el afectado me pida otra cosa (por lo que he comentado antes: si admiten la prueba del usuario, deben admitir la mía). No obstante, siempre hay excepciones. Ahora mismo, se me ocurren dos:

- El medio sea inseguro a todas luces (ejemplo: enviar una historia clínica por email). En estos casos, al menos, tendremos que advertir al usuario de dicha circunstancia.
- Por el contenido de la petición (por ejemplo, el afectado se está poniendo farruco), me interesa contestar por burofax.

Deber de diligencia en la selección de proveedores con acceso a datos personales.

El artículo 28.1 del **Reglamento General de Protección de Datos**, establece que el responsable del tratamiento elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme a los requisitos establecidos en la normativa de protección de datos. De acuerdo con el anterior precepto, los responsables del tratamiento tienen un deber de diligencia a la hora de seleccionar y contratar a un proveedor que vaya a acceder a datos personales en calidad de encargado del tratamiento. El presente documento contiene algunas preguntas que podrán realizarse al proveedor con el que se pretenda externalizar algún servicio. El objetivo de estas preguntas es conocer el grado de cumplimiento del proveedor en materia de protección de datos. Además de las preguntas, se debe solicitar al proveedor cualquier documento que permita acreditar sus respuestas. Por ejemplo, si el proveedor nos dice que sí cuenta con alguna certificación en materia de seguridad, nos debería aportar una copia de la certificación.

***Checklist* previo – Gestión de proveedores.**

ID	Pregunta	Respuesta
1	¿El Proveedor ha nombrado un Delegado de Protección de Datos o una persona que se ocupe las cuestiones de protección de datos dentro de la entidad?	
2	¿El Proveedor mantiene un registro de actividades de tratamiento?	
3	¿El Proveedor cuenta con un departamento / área de seguridad de la información?	
4	¿El Proveedor realiza auditorías periódicas para verificar el grado de cumplimiento en materia de protección de datos?	
5	¿El Proveedor cuenta con alguna certificación de seguridad?	
6	¿El Proveedor o alguna de sus filiales han sido sancionados o inspeccionados por alguna autoridad europea de protección de datos?	
7	¿El Proveedor está adherido a algún código de conducta que marque pautas relativas a protección de datos?	
8	¿El Proveedor dispone de una política o protocolo interno para la gestión de brechas de seguridad?	
9	¿El Proveedor dispone de una metodología escrita para la realización de evaluaciones de impacto (PIAs)?	
10	¿Alguna de las actividades de tratamiento efectuadas por el Proveedor del Servicio por cuenta de la entidad implican tratamiento de datos fuera del Espacio Económico Europeo?	
11	¿Está prevista la subcontratación de algún servicio que implique tratamiento de datos de carácter personal de la entidad?	
12	¿El Proveedor dispone de una política o protocolo interno relativo a la gestión de derechos de los afectados?	

FECHA:
PERSONA QUE COMPLETA EL CHECK LIST:

CONCEPTOS BÁSICOS

RESPONSABLE DEL TRATAMIENTO (ART. 4.7 RGPD)

"La persona física o jurídica, autoridad pública, servicio u otro organismo (1) *que, solo o junto con otros* (2)*, determine* (3) *los fines y medios* (4) *del tratamiento* (5)*; 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".* **Ejemplo: Una ONG es responsable del tratamiento de gestión de personal, gestión de actividades voluntarias, formación de personal, etc.**

1

"La persona física o jurídica, autoridad pública, servicio u otro organismo"

- Hace referencia al tipo de ente que puede ser responsable del tratamiento.
- No existen restricciones en relación con el tipo de ente que puede asumir la función.

2

"solo o junto con otros"

- Varias entidades pueden actuar como responsables del mismo tratamiento a la vez.
- Corresponsables del tratamiento (art. 26 RGPD): cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento.

3

"determine"

- Poder de decisión sobre el tratamiento. Esta capacidad puede emanar de diferentes circunstancias:

- Competencia legal explícita. Cuando el ordenamiento jurídico establece el nombramiento del responsable del tratamiento o dispone el cometido o la obligación de recoger y tratar determinados datos (ej. Un empleador sobre los datos personales relativos a la seguridad social de sus empleados).
- Competencia jurídica implícita. La capacidad de determinar emana de normas jurídicas generales o funciones tradicionales existentes (ej. Un editor respecto a los datos de sus suscriptores).
- Capacidad de influencia de hecho. La responsabilidad del tratamiento se asigna sobre la base de una evaluación de las circunstancias de hecho.

CONCEPTOS BÁSICOS

RESPONSABLE DEL TRATAMIENTO (ART. 4.7 RGPD)

4

"fines y medios"

- La determinación de los **fines** equivale a determinar el "por qué" del tratamiento y trae consigo la consideración de responsable.
- La determinación de los **medios** equivale a determinar el "cómo" del tratamiento. Abarca:
  - Preguntas técnicas y organizativas (ej. Software o hardware utilizado en el tratamiento).
  - Elementos esenciales (como por ejemplo, determinar qué datos deben tratarse o durante cuánto tiempo).

5

"tratamiento"

- Los fines y medios del tratamiento deben estar relacionados con el tratamiento de datos personales, es decir, "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales*" (art. 4.2 RGPD).

CONCEPTOS BÁSICOS

ENCARGADO DEL TRATAMIENTO (ART. 4.8 RGPD)

"la persona física o jurídica, autoridad pública, servicio u organismo que trate datos personales por cuenta del responsable del tratamiento".

Entidad independiente

Organización/ente externa al responsable del tratamiento

Tratar datos personales por cuenta del responsable

Tratamiento de datos en beneficio del responsable del tratamiento.

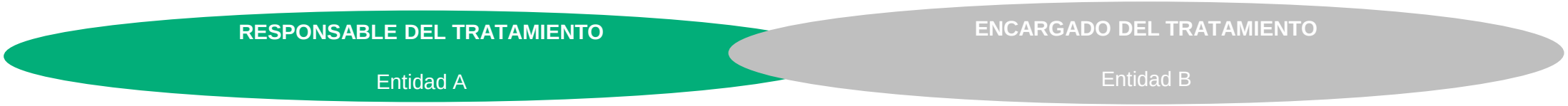
Un mismo ente puede actuar a la vez como responsable del tratamiento para determinadas operaciones de tratamiento y como encargado del tratamiento para otras.

SUBENCARGADO DEL TRATAMIENTO

Subencargado del tratamiento es aquella persona física o jurídica, autoridad pública, servicio u organismo al que el encargado del tratamiento puede recurrir para desarrollar el servicio encomendado por el responsable.

EJEMPLO

Una **entidad A** que tiene muchos empleados firma un contrato con una **entidad B** (empresa de nóminas), para poder pagarles los salarios. La entidad A indica a la entidad B cuándo deben pagarse las nóminas, cuándo un empleado abandona la entidad A o si tiene un aumento de sueldo, y proporciona toda la demás información sobre la nómina y el pago. La entidad B proporciona el sistema informático y conserva los datos de los empleados.



¿Y si la **entidad B** subcontrata el sistema informático con un tercero (**entidad C**) que debe acceder a los datos?

CONTRATACIÓN DE PROVEEDORES: ASPECTOS A TENER EN CUENTA

PROVEEDORES SIN ACCESO A DATOS

Ejemplos:

- ❑ Servicio de limpieza
- ❑ Servicio de reparación de instalaciones

RECOMENDACIONES

Aunque el proveedor no acceda a datos personales, se recomienda incluir una cláusula en los contratos que se tengan suscritos con estos proveedores en la que se regule:

Prohibición de acceso a datos personales.

Obligación de guardar secreto profesional y notificar al responsable en caso de acceso a datos personales.

CONTRATACIÓN DE PROVEEDORES: ASPECTOS A TENER EN CUENTA

PROVEEDORES CON ACCESO A DATOS: ELECCIÓN DEL PROVEEDOR

Artículo 28.1 RGPD:

"Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado".

- El responsable del tratamiento debe evaluar las **suficiencia de las garantías ofrecidas** por el encargado.
- La evaluación debe realizarse de forma **previa**.
- El grado de exhaustividad de la evaluación dependerá de las circunstancias del tratamiento.
- Se puede elaborar un **listado de preguntas** que deben preguntarse al proveedor.
- La evaluación del proveedor exigirá a menudo el **intercambio de la documentación** pertinente (p. ej., la política de privacidad, los términos del servicio, el registro de las actividades de tratamiento, la política de gestión de los registros, la política en materia de seguridad de la información, los informes de las auditorías externas sobre la protección de datos y las certificaciones internacionales reconocidas, como la serie ISO 27000).

Listado de preguntas (*checklist*)

Se adjunta modelo

Informe final

El resultado final puede ser un informe que contenga las conclusiones sobre la idoneidad del encargado del tratamiento y, si procede, la necesidad de exigir garantías adicionales al encargado.

CONTRATACIÓN DE PROVEEDORES: ASPECTOS A TENER EN CUENTA

PROVEEDORES CON ACCESO A DATOS: FORMALIZACIÓN DE LA RELACIÓN CON EL PROVEEDOR

Artículo 28.2 RGPD:

*"El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el **objeto**, la **duración**, la **naturaleza y la finalidad del tratamiento**, el **tipo de datos personales** y **categorías de interesados**, y las **obligaciones y derechos del responsable**".*

- El contrato u acto jurídico puede ser un contrato independiente o incluirse como cláusula/anexo al contrato principal que se tenga con el proveedor.
- El artículo 28.3 del RGPD establece las obligaciones y derechos que debe recoger el contrato/cláusula de encargado de tratamiento:

CONTRATACIÓN DE PROVEEDORES: ASPECTOS A TENER EN CUENTA

PROVEEDORES CON ACCESO A DATOS: FORMALIZACIÓN DE LA RELACIÓN CON EL PROVEEDOR

A. INSTRUCCIONES DEL RESPONSABLE DEL TRATAMIENTO. Identificación de forma clara y precisa de los tratamientos de datos a realizar por parte del encargado del tratamiento. Si el encargado considera que una instrucción infringe la normativa de protección de datos, debe informar al responsable.

B. DEBER DE CONFIDENCIALIDAD. Establecer cómo el encargado garantizará que las personas que accederán a los datos mantendrán la confidencialidad. El cumplimiento de esta obligación debe quedar documentado y a disposición del responsable tratamiento.

C. MEDIDAS DE SEGURIDAD. Corresponde al responsable del tratamiento realizar una evaluación de riesgos para determinar las medidas de seguridad apropiadas. La determinación de las medidas de seguridad puede realizarse a través de una lista exhaustiva, remisión a un estándar o marco nacional o internacional reconocido.

D. RÉGIMEN DE SUBCONTRATACIÓN. El RGPD exige la autorización previa por escrito del responsable del tratamiento que puede ser general o específica. El subencargado del tratamiento debe estar sujeto a las mismas condiciones que el encargado del tratamiento.

E. DERECHOS DE LOS INTERESADOS. El contrato de encargado del tratamiento debe establecer si corresponde al encargado del tratamiento atender las solicitudes de los derechos o bien establecer expresamente que su única obligación es comunicar al responsable las peticiones que puede recibir.

F. COLABORACIÓN EN EL CUMPLIMIENTO DE LAS OBLIGACIONES DEL RESPONSABLE. Se debe establecer que el encargado ayudará a garantizar al responsable: (i) la aplicación de las medidas de seguridad; (ii) la notificación de violaciones de datos tanto a las autoridades de control como a los interesados; (iii) la realización de evaluaciones de impacto, y; (iv) las consultas previas a las autoridades de control.

G. EL DESTINO DE LOS DATOS AL FINALIZAR LA PRESTACIÓN Se puede optar por: (i) supresión de los datos por parte del encargado, o; (ii) la devolución de los datos personales y de cualquier copia existente. No obstante, el encargado puede conservar una copia con los datos debidamente bloqueados.

H. COLABORACIÓN CON EL RESPONSABLE PARA DEMOSTRAR EL CUMPLIMIENTO. Es preciso establecer la obligación del encargado de poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento.

OTRAS CUESTIONES GENERALES

¿Qué tratamientos puede llevar a cabo un encargado sobre los datos personales que acceda del responsable?

El encargado puede realizar todos los tratamientos, automatizados o no, que el responsable del tratamiento le haya encomendado formalmente.

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.

¿ Qué nivel de decisión puede asumir un encargado del tratamiento?

El encargado del tratamiento puede adoptar todas las decisiones organizativas y operacionales necesarias para la prestación del servicio que tenga contratado. En ningún caso puede variar las finalidades y los usos de los datos ni los puede utilizar para sus propias finalidades.

¿Quién es el responsable de los tratamientos realizados por el encargo?

El responsable del tratamiento no pierde esta consideración en ningún caso, y por tanto, continúa siendo responsable del correcto tratamiento de los datos personales. Además, tiene una obligación de especial diligencia en la elección y supervisión del encargado.

OTRAS CUESTIONES GENERALES

¿Proveedores fuera del Espacio Económico Europeo?

Si el encargado del tratamiento se encuentra fuera del EEE, el RGPD seguirá siendo de aplicación si el responsable del tratamiento tiene su sede en la Unión Europea.

Espacio Económico Europeo comprende:
Unión Europea, Noruega, Islandia y Liechtenstein.

Además, se deberá tener en cuenta que la comunicación de datos constituye una transferencia internacional de datos en el marco del contrato de encargo.

Adaptación de contratos del Encargado del Tratamiento antes del RGPD

Los contratos de encargo formalizados antes de la plena aplicabilidad del RGPD (25 de mayo de 2018) se deben de adaptar para respetar lo establecido en el artículo 28 RGPD. No obstante:

Disposición transitoria quinta de la LOPDGDD

a. Contratos con duración determinada
Los contratos y acuerdos establecidos antes de 25 de mayo de 2018 mantienen su vigencia hasta la fecha de vencimiento.

b. Contratos con duración indefinida
Mantienen la vigencia hasta el 25 de mayo de 2022.

OTRAS CUESTIONES GENERALES

Herramientas y modelos

Directrices de la AEPD y modelo de contrato

ANEXO I

Ejemplo de cláusulas contractuales para supuestos en que el encargado del tratamiento trate los datos en sus locales y exclusivamente con sus sistemas

(Estas cláusulas tienen sólo carácter orientativo y deben adaptarse a las circunstancias concretas del tratamiento que se lleve a cabo)

1. Objeto del encargo del tratamiento

Mediante las presentes cláusulas se habilita a la entidad ....., encargada del tratamiento, para tratar por cuenta de ....., responsable del tratamiento, los datos de carácter personal necesarios para prestar el servicio de ..... .

El tratamiento consistirá en: *(descripción detallada del servicio)*

Concreción de los tratamientos a realizar:

☐ Recogida	☐ Registro
☐ Estructuración	☐ Modificación
☐ Conservación	☐ Extracción
☐ Consulta	☐ Comunicación por transmisión
☐ Difusión	☐ Interconexión
☐ Cotejo	☐ Limitación
☐ Supresión	☐ Destrucción
☐ Conservación	☐ Comunicación

☐ Otros:.....

Modelo contrato Comisión Europea

L 199/18 ES Diario Oficial de la Unión Europea 7.6.2021

DECISIÓN DE EJECUCIÓN (UE) 2021/915 DE LA COMISIÓN

de 4 de junio de 2021

relativa a las cláusulas contractuales tipo entre responsables y encargados del tratamiento contempladas en el artículo 28, apartado 7, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo y en el artículo 29, apartado 7, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el 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 («RGPD») (1), y en particular su artículo 28, apartado 7,

Visto el Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (2), y en particular su artículo 29, apartado 7,

Considerando lo siguiente:

(1) Los conceptos de responsable y encargado del tratamiento desempeñan un papel crucial en la aplicación del Reglamento (UE) 2016/679 y del Reglamento (UE) 2018/1725. El «responsable del tratamiento» o «responsable» es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento. A efectos del Reglamento (UE) 2018/1725, se entiende por responsable del tratamiento la institución o el organismo o la dirección general u otra entidad organizativa de la Unión que, por sí sola o conjuntamente con otros, determine los fines y medios del tratamiento de datos personales. Cuando los fines y medios de ese tratamiento se determinen en un acto específico de la Unión, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser establecidos por la Unión. El «encargado del tratamiento» o «encargado» es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

(2) Debe aplicarse el mismo conjunto de cláusulas contractuales tipo a la relación entre los responsables y los encargados del tratamiento sujetos al Reglamento (UE) 2016/679 y también cuando estén sujetos al Reglamento (UE) 2018/1725. Esto se justifica porque, en aras de un planteamiento coherente de protección de los datos personales en la Unión y de la libre circulación de datos personales en toda la Unión, las normas de protección de datos del Reglamento (UE) 2016/679, aplicables al sector público en los Estados miembros, y las normas de protección de datos del Reglamento (UE) 2018/1725, aplicables a las instituciones, órganos y organismos de la Unión, se armonizaron en la medida de lo posible.

(3) Con el fin de asegurar que se cumplan los requisitos del Reglamento (UE) 2016/679 y el Reglamento (UE) 2018/1725, cuando se encomienden actividades de tratamiento a un encargado, el responsable debe recurrir únicamente a encargados que ofrezcan garantías suficientes, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del Reglamento (UE) 2016/679 y del Reglamento (UE) 2018/1725, incluida la seguridad del tratamiento.

(4) El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o del Estado miembro, que vincule al encargado respecto del responsable y establezca los elementos enumerados en el artículo 28, apartados 3 y 4, del Reglamento (UE) 2016/679 o en el artículo 29, apartados 3 y 4, del Reglamento (UE) 2018/1725. Dicho contrato o acto deberá recogerse por escrito; se puede hacer en formato electrónico.

(5) De conformidad con el artículo 28, apartado 6, del Reglamento (UE) 2016/679 y el artículo 29, apartado 6, del Reglamento (UE) 2018/1725, el responsable y el encargado pueden optar entre, bien negociar un contrato individual que contenga los elementos obligatorios establecidos en el artículo 28, apartados 3 y 4, del Reglamento (UE) 2016/679 o en el artículo 29, apartados 3 y 4, del Reglamento (UE) 2018/1725, respectivamente, bien utilizar, total o parcialmente, las cláusulas contractuales tipo fijadas por la Comisión con arreglo al artículo 28, apartado 7, del Reglamento (UE) 2016/679 y al artículo 29, apartado 7, del Reglamento (UE) 2018/1725.

(1) DO L 119 de 4.5.2016, p. 1.
(2) DO L 295 de 21.11.2018, p. 39.

GUÍA PARA LA ADAPTACIÓN DE UNA PÁGINA WEB

1. Conceptos básicos

❑ Textos necesarios

Cualquier página web necesita incluir ciertos textos legales para cumplir con la normativa. En función del tipo de web y actividad del responsable de la web, será necesarios unos u otros. Con carácter general, una página web deberá contener los siguientes textos legales:

- Aviso legal / Términos y condiciones
- Política de privacidad y cláusulas informativas
- Política de cookies

❑ Marco legal

A la hora de redactar los textos indicados en el apartado anterior debemos tener en cuenta la normativa aplicable para cada uno de los mismos:

- 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 **(RGPD)**: link
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales **(LOPDGDD)**: link
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico **(LSSI)**: link
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias **(Ley de Consumidores y Usuarios)**: link

❑ Otros materiales de apoyo

Adicionalmente a la normativa mencionada en el apartado anterior, para la adaptación de una página web son de utilidad las siguientes guías disponibles en la página web de la Agencia Española de Protección de Datos (AEPD):

- **Guía para el cumplimiento del deber de informar:** link
- **Guía de cookies:** link

2. Caso práctico

Para la sesión del 12 de mayo, tenéis disponibles en el apartado del Taller 5 “Adaptación de páginas web” de la páginas web de la Fundación Pro Bono España y de la Coordinadora de ONGD de la Región de Murcia los modelos que debéis completar.

A continuación, os contamos cómo debéis adaptarlos para tener una página web que cumpla con la normativa:

❑ ADAPTACIÓN DE AVISO LEGAL Y TÉRMINOS Y CONDICIONES DE USO Y VENTA

- **Materiales:**
  - Modelo de Aviso Legal y T&C de Uso y Venta
  - Normativa: LSSI, Ley de Consumidores y Usuarios
- **Información práctica:**

El modelo facilitado contiene en un mismo documento el aviso legal y los términos y condiciones de uso y venta.

Siguiendo este modelo, el **aviso legal corresponde a la cláusula 2 del modelo** y deberá completarse con la siguiente información mínima de la entidad (artículo 10 de la LSSI):

- **Nombre o denominación social**;
- **Residencia o domicilio;**
- **Correo electrónico u otros datos de contacto**;
- **NIF**;
- **Datos de inscripción en el Registro correspondiente (Registro Mercantil, de Fundaciones...).**

Adicionalmente, se podrá incluir (cuando sea de aplicación) la siguiente información:

- Si fuera necesaria autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión;
- Ciertos datos si ejerce una profesión regulada (e.g. datos del Colegio profesional) y
- Los códigos de conducta a los que se esté adherido y la manera de consultarlos electrónicamente.

Todas las cláusulas (excepto la 8) del modelo corresponden a los términos y condiciones de uso del sitio web, que deberán adaptarse al propio sitio web de la entidad.

La **cláusula 8 del modelo corresponde a los términos y condiciones de venta del sitio web**. Esta cláusula únicamente deberá incluirse cuando la entidad comercialice productos o servicios a través de su página web. Para completarla se deberá incluir el proceso de compra online de la entidad teniendo en cuenta las obligaciones señaladas en la Ley de Consumidores y Usuarios (en particular, los arts. 60 y ss.), entre otras, en relación con los productos, el precio, el pago, la entrega y las devoluciones, tal y como se señala en las correspondientes cláusulas del modelo.

❑ ADAPTACIÓN DE LA POLÍTICA DE PRIVACIDAD Y FORMULARIOS WEB

- **Materiales**:
  - Modelo de Política de Privacidad: El modelo y la guía de cómo completarlo están disponibles en el Taller 2 “Cómo redactar una Política o cláusula informativa de privacidad”.
  - Normativa y recomendaciones: Artículos 13 y 14 RGPD, Guía de la AEPD para el cumplimiento del deber de informar.
- **Información práctica:**

Si bien la **política de privacidad** y las **cláusulas informativas** fueron objeto del Taller 2, estas deberán incluirse en la página web siempre que se trate algún dato personal, como por ejemplo:

- El registro de la IP por alguna cookie de terceros alojada en la web, o
- A través de un formulario de contacto (en el que se suelen pedir nombre y datos de contacto).

Por ello, para la segunda sesión del taller deberéis tener correctamente adaptada la política de privacidad siguiendo el modelo del Taller 2, y publicarla en la página web de la entidad de manera que esté visible; por ejemplo, a través de un hipervínculo al final de la página web que redirija a la política de privacidad.

Asimismo, los formularios web (p.ej. de registro de cuenta, de contacto, suscripción a *newsletters*, etc.) deberán incluir las correspondientes casillas no pre-marcadas para cumplir con el deber de información y consentimiento:

☐ He leído y acepto los términos y condiciones y la política de privacidad.

☐ Consiento la recepción de comunicaciones por cualquier medio electrónico de [completar nombre de la ONG] con fines comerciales. (SOLAMENTE INCLUIR LA SEGUNDA EN EL CASO DE QUE SE ENVÍEN COMUNICACIONES COMERCIALES)

- **ADAPTACIÓN DE COOKIES**

  - **Materiales**:
    - Modelo Primera Capa: Banner y Panel de Configuración de cookies.
    - Modelo Segunda Capa: Política de cookies.
    - Normativa y recomendaciones: LSSI y Guía de cookies de la AEPD.
  - **Información práctica:**

Se han elaborado dos modelos para la adaptación de las cookies siguiendo las recomendaciones de la AEPD. De esta manera para cumplir con el deber de información y obtener adecuadamente el consentimiento de los usuarios, la entidad debe ofrecer a los usuarios de su página web la información en dos capas:

- Primera capa: Banner y Panel de configuración de cookies
- Segunda capa: Política de cookies

PRIMERA CAPA:

El Banner es el aviso informativo de cookies que deberá aparecer en el momento en el que el usuario empiece a navegar en el sitio web, por el que se deberá informar al usuario con un lenguaje claro y sencillo, de forma concisa, transparente, inteligible y de fácil acceso:

- Esta información se facilitará antes del uso de las cookies, a través de un formato que sea visible para el usuario y que deberá mantenerse hasta que el usuario realice la acción requerida para la obtención del consentimiento o su rechazo.
- Si no se pulsa el botón “Aceptar”, el usuario no autoriza el uso de cookies (por lo tanto, no está legitimado el uso de cookies si el usuario no pulsa el botón para aceptar cookies y simplemente continúa navegando o permanece en la web).
- Si se pulsa el botón “Configurar”, el usuario deberá ser redirigido al “Panel de configuración de cookies”.
- Como regla general, siempre que un consentimiento haya sido obtenido de forma válida, no será necesario obtenerlo cada vez que un usuario visite de nuevo la misma página web desde la que se presta el servicio. No obstante, la AEPD considera buena práctica que la validez del consentimiento del usuario para el uso de una cookie no tenga una duración superior a 24 meses. Por lo tanto, os recomendamos que **durante este tiempo conservéis la selección realizada** por el usuario sobre sus preferencias y **volváis a mostrarle el aviso (para solicitar un nuevo consentimiento) una vez transcurridos los 24 meses**.
- En todo caso, si los fines de uso de las cookies o los terceros que hacen uso de las cookies cambian después de haber obtenido el consentimiento, será necesario actualizar la política de cookies y permitir a los usuarios tomar una nueva decisión.

El Panel de Configuración de cookies deberá adaptarse en función del tipo de cookies que se utilizan en la página web. Las cookies se pueden agrupar por tipología realizando una descripción de las mismas, incluyendo la finalidad y especificar a modo listado las diferentes cookies (p.ej. Google Analytics) que se utilizan dentro de esa tipología (p.ej. cookies analíticas). Para ello, podéis seguir la estructura de la tabla que os hemos indicado como modelo. Para que el consentimiento sea válido, las pestañas de configuración deberán estar siempre inactivas, a excepción de aquellas cookies que no necesiten consentimiento (como las técnicas) que podrán estar siempre activas.

SEGUNDA CAPA:

La Política de cookies debe completarse siguiendo el modelo facilitado con la siguiente información mínima indicada en la Guía de cookies.

- **Definición y función genérica** de las cookies.
- **Tipo de cookies** que se utilizan en la web y su finalidad.
- **Quién utiliza las cookies** (esto es, si la información obtenida por las cookies es tratada solo por el editor y/o también por terceros con los que editor haya contratado la prestación de un servicio para el cual se requiera el uso de cookies).
- **Forma de aceptar, denegar o revocar el consentimiento para el uso de cookies** enunciadas a través de las funcionalidades facilitadas por el editor (el sistema de gestión o configuración de cookies que se haya habilitado) o a través de las plataformas comunes que pudieran existir para esta finalidad.
- Si las hubiera, **información sobre las transferencias de datos a terceros países realizadas por el editor**.
- Cuando la **elaboración de perfiles** implique la toma de decisiones automatizadas con efectos jurídicos para el usuario o que le afecten significativamente de modo similar, será necesario que se informe sobre la **lógica utilizada, así como la importancia y las consecuencias previstas** de dicho tratamiento para el usuario.
- **Periodo de conservación** de los datos para los diferentes fines.
- En relación con el resto de información exigida por el artículo 13 del RGPD que no se refiera de forma específica a las cookies (por ejemplo, los derechos de los interesados), **el editor podrá remitirse a la política de privacidad.**

❑ CUESTIONES PRÁCTICAS PARA LA ADAPTACIÓN DE UNA WEB

Para implementar correctamente los textos en vuestra página web, deberéis cumplir con lo siguiente:

- **Enlaces visibles y fácilmente accesibles (en la página de inicio de la web)**
- Información en **español** si el público está en España
- Necesidad de **actualización** constante de los textos legales.

¿Qué textos legales necesito incluir en mi página web?

Cualquier página web necesita incluir ciertos textos legales para cumplir con la normativa. En función del tipo de web y actividad del responsable de la web, será necesarios unos u otros.

En este caso, estos documentos no solamente se exigen en la normativa de protección de datos (RGPD y LOPDGDD) sino también en otras normas como la LSSI y ley de consumidores y usuarios.

Textos necesarios

- Aviso legal / Términos y condiciones
- Política de privacidad
- Política de cookies

Marco legal a tener en cuenta

- RGPD y LOPDGDD
- LSSI
- Ley de Consumidores y Usuarios
- Guías de la AEPD

AVISO LEGAL

El **Aviso legal** no es un concepto legal definido en la normativa.

Lo que se define en la normativa es la **información mínima** que debe incluirse en la medida en que se es "prestador de servicios de la sociedad de la información" según la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).

¿Cuándo se prestan **servicios de la sociedad de la información**?

LSSI:

"*todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.*
El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios."

El concepto de "servicios de la sociedad de la información" es muy amplio e incluye no solo la contratación de bienes o servicios por vía electrónica sino también el **suministro de información por vía telemática siempre que represente una actividad económica (directa o indirectamente)**. Ello incluye la actividad de las entidades sociales u ONGs.

AVISO LEGAL

Contenido mínimo obligatorio (art. 10 de la LSSI), a facilitarse por **medios electrónicos, de forma permanente, fácil, directa y gratuita:**

- ❑ **Nombre o denominación social**
- ❑ **Residencia o domicilio**
- ❑ **Correo electrónico u otros datos de contacto**
- ❑ **NIF**
- ❑ **Datos de inscripción en el Registro correspondiente (Registro Mercantil, de Fundaciones...)**
- ❑ **Si fuera necesaria autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.**
- ❑ **Ciertos datos si ejerce una profesión regulada (e.g. datos del Colegio profesional)**
- ❑ **Códigos de conducta a los que se esté adherido y la manera de consultarlos electrónicamente.**

TÉRMINOS Y CONDICIONES (DE USO)

Los **términos y condiciones** suelen incluirse junto con el Aviso Legal o bien en un texto separado.

En ellos se establecen: (i) las condiciones de acceso y uso de la web y (i) si hubiera comercio electrónico, las condiciones de venta.

Las condiciones de **acceso y uso** de la web **no son obligatorias pero sí muy recomendables** y en la práctica suelen incluir:

Prohibiciones de uso por parte del usuario: No utilizar la web con fines ilícitos o prohibidos por la normativa

Responsabilidad y exoneración de responsabilidad

Propiedad Intelectual e Industrial

Otros términos de uso de la web (e.g. si es necesario el registro)

TÉRMINOS Y CONDICIONES (DE VENTA)

Las condiciones de **venta** se incluyen si a través de la web hay **comercio electrónico** (productos/servicios). La Ley de Consumidores y Usuarios (Real Decreto Legislativo 1/2007) exige que figure cierta información para garantizar la protección del consumidor y usuario, tales como:

Las características principales de los bienes o servicios

El precio total, incluidos todos los impuestos y tasas

El derecho a devoluciones y desistimiento comercial

Los procedimientos de pago, entrega, ejecución y la fecha en que el vendedor se compromete a entregar el producto o servicio

La existencia, cuando proceda, de asistencia técnica y servicios posventa, garantías comerciales

POLÍTICA DE PRIVACIDAD

Cualquier página web debe incluir una **política de privacidad** siempre que la página o sitio web recopile algún **dato de carácter personal**, por ejemplo:

El registro de la IP por alguna cookie de terceros alojada en la web o

A través de un formulario de contacto (en el que se suelen pedir nombre y datos de contacto).

Contenido obligatorio como recordatorio del **TALLER 2** (**artículos 13 y 14 RGPD**):

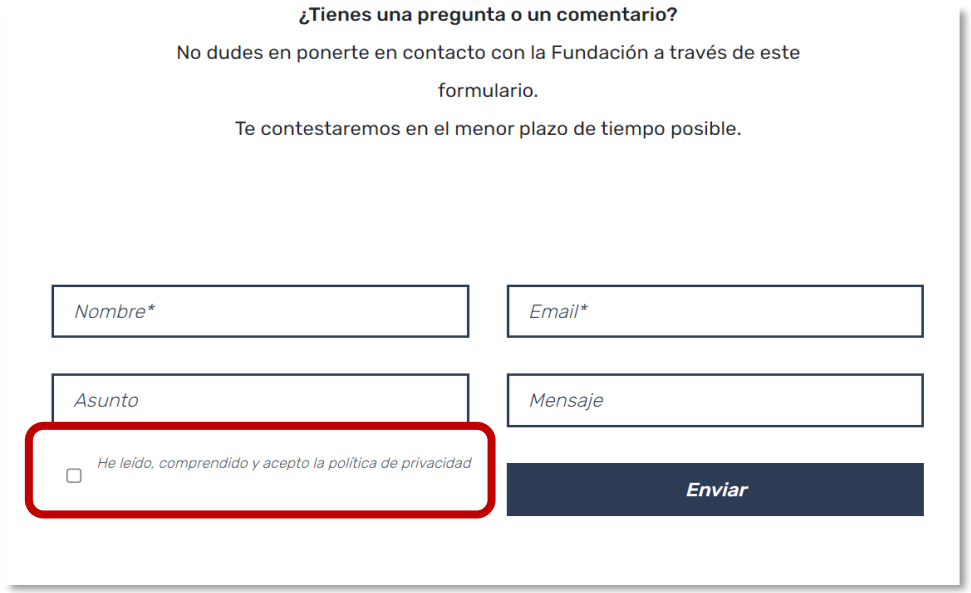
- ❑ Identidad y datos de contacto del responsable del tratamiento
- ❑ Finalidad/es del tratamiento y su/s base/s jurídica/s/ legitimación
- ❑ Destinatarios de los datos personales (si se quieren ceder los datos a un tercero).
- ❑ Posibilidad de realizar transferencias internacionales de datos (caso en que los datos salen fuera del EEE)
- ❑ Plazo de conservación de los datos o criterios utilizados para determinar el plazo.
- ❑ Derechos del interesado y datos de contacto del DPD o, si no lo hubiera, de quien se encargue de gestionar las cuestiones de protección de datos.
- ❑ Derecho a presentar una reclamación ante una autoridad de control cuando no hayas obtenido satisfacción en el ejercicio de tus derechos
- ❑ Categorías de datos personales de que se trate (e.g. datos de identificación, de contacto)
- ❑ Fuente de la que proceden los datos (e.g. del formulario de contacto web de la entidad)
- ❑ Existencia de decisiones automatizadas (elaboración de perfiles). En estos casos, dar información significativa sobre (i) la lógica aplicada y (ii) la importancia y las consecuencias previstas de dicho tratamiento para el interesado

ADAPTACIÓN DE FORMULARIOS WEB

Si hay formularios web de contacto o suscripción, añadir las **siguientes casillas NO PRE-MARCADAS:**

☐ **He leído y acepto los términos y condiciones y la política de privacidad (OBLIGATORIA ACEPTACIÓN)**

☐ **Consiento la recepción de comunicaciones por cualquier medio electrónico de [completar nombre de la ONG] con fines comerciales. (PROBABLEMENTE NO SERÁ NECESARIO EN EL CASO DE UNA ONG). Art. 22.1 de la LSSI.**



POLÍTICA DE COOKIES

En caso de que se utilicen cookies o tecnologías similares en una web, debe incluirse una **política de cookies**. Se regula en:

La LSSI	La Guía de cookies de la AEPD

El Art. 22 de la LSSI requiere **consentimiento + información** para su utilización:

"*Los prestadores de servicios podrán utilizar* ***dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización****, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*"

La Guía de cookies establece cómo debe obtenerse el consentimiento y cómo debe facilitarse la información (mediante dos capas).

La Política de cookies se divide en:

Primera capa con un banner y un panel de configuración	Segunda capa mediante la Política de Cookies

POLÍTICA DE COOKIES – PRIMERA CAPA

Primera capa – Información en el banner acompañado por el panel de configuración

Editor responsable del sitio web. No será necesaria la denominación social, siempre que sus datos identificativos completos figuren en otras secciones del sitio web (aviso legal, política de privacidad, etc.) y su identidad pueda desprenderse de forma evidente del propio sitio web.

Finalidades de las cookies que se utilizarán.

Información sobre **si las cookies son propias (del responsable de la página web) o también de terceros** asociados a él, sin que sea necesario identificar a los terceros en esta primera capa.

Información genérica sobre el tipo de datos que se van a recopilar y utilizar en caso de que se elaboren perfiles de los usuarios (por ejemplo, cuando se utilicen cookies de publicidad comportamental).

Modo en el que el usuario puede aceptar, configurar y rechazar la utilización de cookies, con la advertencia, en su caso, de que si se realiza una determinada acción, se entenderá que el usuario acepta el uso de las cookies.

Un **enlace claramente visible dirigido a una segunda capa informativa en la que se incluya una información más detallada**, utilizando, por ejemplo, el término “Cookies”, “Política de cookies” o “Más información, pulsa aquí”.

POLÍTICA DE COOKIES – SEGUNDA CAPA

Segunda capa – Información incluida en un enlace de la web

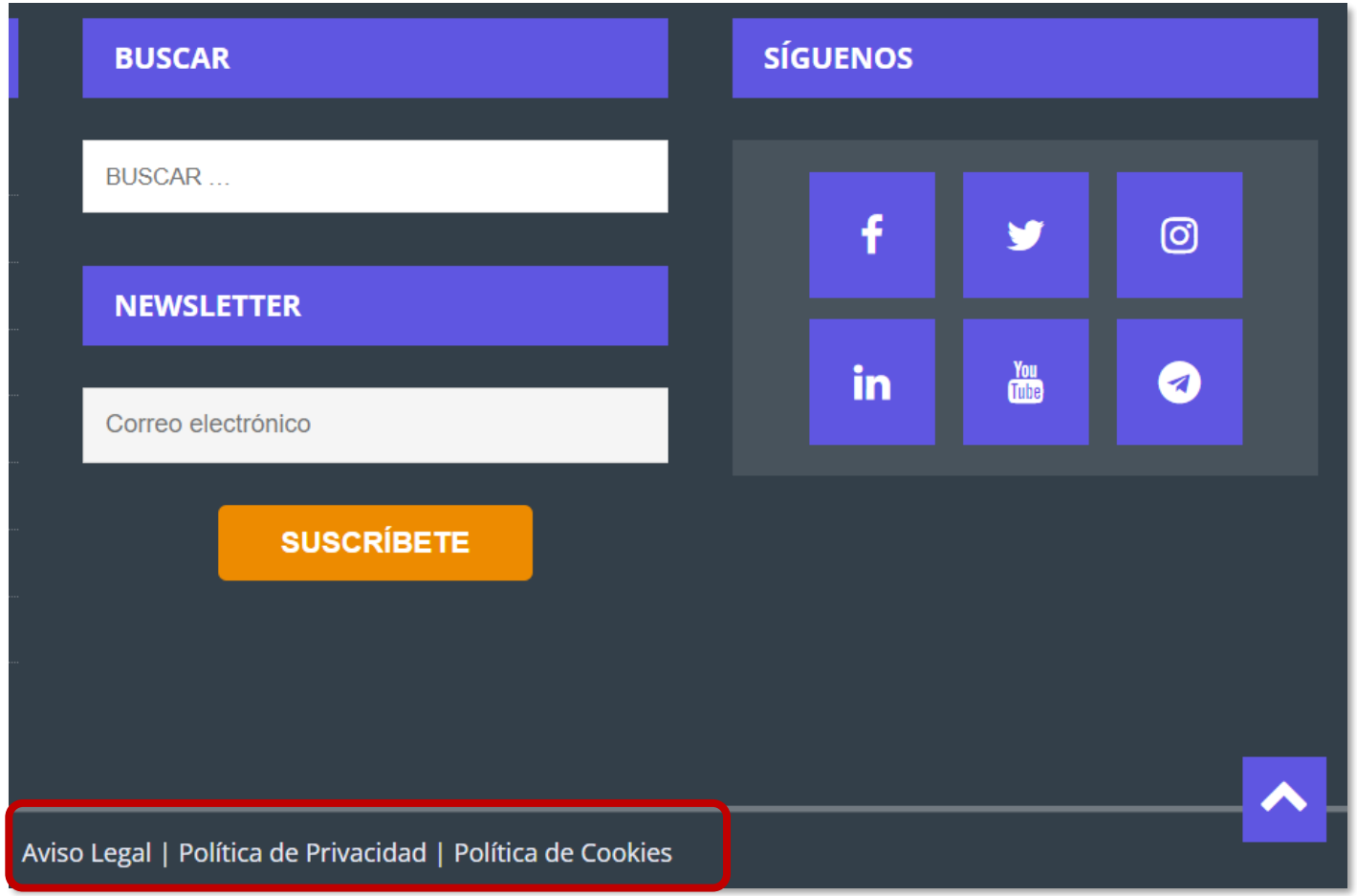
Definición y **función genérica de las cookies.**	**Tipo de cookies** que se utilizan en la web y su finalidad	**Quién utiliza las cookies** (esto es, si la información obtenida por las cookies es tratada solo por el editor y/o también por terceros con los que editor haya contratado la prestación de un servicio para el cual se requiera el uso de cookies)	**Forma de aceptar, denegar o revocar el consentimiento para el uso de cookies** enunciadas a través de las funcionalidades facilitadas por el editor (el sistema de gestión o configuración de cookies que se haya habilitado) o a través de las plataformas comunes que pudieran existir para esta finalidad.
Si las hubiera, **información sobre las transferencias de datos a terceros países realizadas por el editor**.	Cuando la **elaboración de perfiles** implique la toma de decisiones automatizadas con efectos jurídicos para el usuario o que le afecten significativamente de modo similar, será necesario que se informe sobre la **lógica utilizada, así como la importancia y las consecuencias previstas** de dicho tratamiento para el usuario.	**Periodo de conservación** de los datos para los diferentes fines.	En relación con el resto de información exigida por el artículo 13 del RGPD que no se refiera de forma específica a las cookies (por ejemplo, los derechos de los interesados), **el editor podrá remitirse a la política de privacidad.**

CUESTIONES PRÁCTICAS

Enlaces **visibles y fácilmente accesibles** (en la página de inicio de la web)

Información en **español** si el público está en España

Necesidad de **actualización**



POSIBLES SANCIONES

Apercibimiento, una prohibición temporal o definitiva del tratamiento y una multa de hasta 20 millones de euros o un 4 % del volumen de negocio total anual mundial (RGPD).

Multas de hasta 600.000 euros (LSSI) en casos muy graves.

¡CUIDADO CON LAS COOKIES! Multa de 30.000 euros a Iberia:

Si no se pulsaba el botón de “aceptar” o el botón de “configuración de cookies”, no se permitía seguir navegando, con lo que no se daba la opción al usuario de rechazar el uso de cookies.

La segunda capa de cookies no identificaba las cookies de terceros ni el periodo de conservación de las cookies.


Protección de Datos multa a Iberia por incumplir la política de cookies en su web

Aviones Iberia

TALLER 6: OTRAS SITUACIONES CONFLICTIVAS COMUNES. ENVÍO DE COMUNICACIONES COMERCIALES. NOMBRAMIENTO DEL DPO

1.-Envío de comunicaciones comerciales

a) ¿Qué es una comunicación comercial?
b) ¿Por qué medios se pueden enviar las comunicaciones comerciales?
c) ¿En qué casos se pueden enviar las comunicaciones comerciales?
d) Supuestos específicos

2.-Eldelegado de protección de datos

a) ¿Qué es un delegado de protección de datos?
b) ¿Cuáles son sus funciones?
c) ¿Qué requisitos debe reunir?
d) ¿Es obligatorio nombrarlo?
e) ¿Debe comunicarse su nombramiento a la AEPD?

3.-Materiales

- Reglamento General de Protección de Datos: https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32016R0679
- Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673
- Ley de servicios de la sociedad de la información y de comercio electrónico: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
- Ley General de Telecomunicaciones: https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950
- Directrices sobre delegados de protección de datos (DPD), adoptadas el 13 de diciembre de 2016 por el antiguo Grupo de Trabajo del Artículo 29
- Preguntas frecuentes de la AEPD sobre la figura del delegado de protección de datos: https://www.aepd.es/es/preguntas-frecuentes/4-responsable-encargado-y-dpd/1-delegado-de-proteccion-de-datos#:~:text=%C2%BFQu%C3%A9%20es%20un%20Delegado%20de,en%20el%20responsable%20o%20encargado.

4.-Instrucciones para completar los modelos

Junto con la presentación de la clase del jueves 19 de mayo se ha facilitado un modelo de informe para analizar la necesidad de nombrar a un delegado de protección de datos. De cara a la próxima sesión, os pedimos que completéis el modelo de informe en base a los tratamientos de datos personales que realizáis en vuestra entidad para que así podáis llegar a la conclusión de si es necesario que nombréis a un delegado de protección de datos. Como comentamos en la última sesión, aunque la conclusión sea que no es necesario nombrarlo, tener un estudio completado ayuda a cumplir con el principio de responsabilidad proactiva. Además de corregir el trabajo que hayáis realizado, podemos aprovechar la próxima sesión para comentar dudas sobre el envío de comunicaciones comerciales.

Sònia Sebé y Manel Santilari. Clifford Chance.

Envío de newsletters y comunicaciones comerciales: ¿Qué es una comunicación comercial?

- Anexo Ley 34/2002 apartado f)
  - Toda forma de comunicación dirigida a la promoción, directa o indirecta, de la imagen o de los bienes o servicios de una empresa, organización o persona que realice una actividad comercial, industrial, artesanal o profesional

Envío de newsletters y comunicaciones comerciales: ¿Por qué medios se pueden enviar las comunicaciones comerciales?

- Medios electrónicos:
  - Correo electrónico
  - SMS
  - WhatsApp
- Medios no electrónicos:
  - Correo postal
  - Llamada
- Comunicaciones comerciales que no implican un tratamiento de datos personales:
  - Distribución de folletos
  - Banners publicitarios en sitio web

Envío de newsletters y comunicaciones comerciales: Supuestos específicos

- Aceptar la política de privacidad en la que se incluye la posibilidad de enviar comunicaciones comerciales (basadas en el consentimiento) no es suficiente. Se requiere un consentimiento autónomo
- Enviar una comunicación informando de la posibilidad de participar en un sorteo también es una comunicación comercial
- El hecho de incluir mensajes promocionales en un sobre que contiene información contractual se considera una comunicación comercial
- Enviar un correo electrónico durante la pandemia informando de que pueden realizarse operaciones bancarias de forma no presencial es una comunicación comercial

Envío de newsletters y comunicaciones comerciales: ¿En qué casos se pueden enviar las comunicaciones comerciales?

- Medios electrónicos (Artículo 21 Ley 34/2002)
  - Regla general: consentimiento previo del destinatario
  - Excepción al consentimiento: cuando exista una **relación contractual previa**, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales **referentes a productos o servicios de su propia empresa** que sean **similares a los que inicialmente fueron objeto de contratación** con el cliente

  Deberá ofrecerse al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito (p.ej. correo electrónico, enlace, etc.), tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija

  Consentimiento deberá cumplir con lo dispuesto en el artículo 7 RGPD

  Obligaciones de información (artículo 13 RGPD)

- Medios no electrónicos – correo postal (RGPD)
  - Regla general: consentimiento previo del destinatario
  - Excepción al consentimiento: concurrencia de un interés legítimo Cuando exista una **relación contractual previa**, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales **referentes a productos o servicios de su propia empresa** que sean **similares a los que inicialmente fueron objeto de contratación** con el cliente

  Deberá ofrecerse al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales

- Medios no electrónicos – llamada telefónica
  - Artículo 23.4 LOPDGDD – obligación de consultar los sistemas de exclusión publicitaria
  - Artículo 48.1 LGT – derecho de oposición a recibir llamadas no deseadas con fines de comunicación comercial
  - Artículo 69 Real Decreto 424/2005 – distinción entre llamadas no solicitadas efectuadas mediante sistemas de llamada automática sin intervención humana y llamadas efectuadas mediante otros sistemas

El delegado de protección de datos: ¿qué es un delegado de protección de datos?

- Figura que, dentro de una empresa (responsable o encargado del tratamiento) se encarga de que la empresa en cuestión cumpla con la normativa de protección de datos
- Cualquier responsabilidad por posibles incumplimientos de la normativa recaerá sobre el responsable / encargado del tratamiento, no sobre el DPD
- Puede designarse a un único DPD por grupo empresarial, si es "*fácilmente accesible desde cada establecimiento*"
- El DPD puede ser interno o externo
- Regulación: artículos 37 a 39 RGPD y 34 a 37 de la LOPDGDD

El delegado de protección de datos: ¿cuáles son sus funciones?

- Informar, asesorar y supervisar al responsable / encargado del tratamiento en relación con las obligaciones correspondientes en virtud de la normativa de protección de datos
- Cooperación con la autoridad de control y punto de contacto de la misma
- Función de soporte a los interesados: resolución de dudas y reclamaciones

El delegado de protección de datos: ¿qué requisitos debe reunir?

- ❑ Debe tener conocimientos especializados en protección de datos
  - Posibilidad de demostrar estos conocimientos mediante la certificación de DPD
  - Las entidades de certificación acreditadas por la Entidad Nacional de Acreditación (ENAC) otorgaran al profesional un certificado que implica un reconocimiento de que tiene las competencias adecuadas para el desarrollo de las funciones del DPD: **https://www.enac.es/web/enac/entidades-acreditadas/buscador-de-acreditados**
- ❑ Debe integrarse en la organización de modo que pueda desplegar su actividad de forma eficiente
- ❑ Debe contar con el respaldo de la dirección y disponer de los recursos materiales adecuados
- ❑ Debe asegurarse su independencia de criterio (no se le puede sancionar como consecuencia del desempeño de sus funciones)

El delegado de protección de datos: ¿es obligatorio nombrarlo?

- ❑ Depende
- ❑ Carácter obligatorio siempre que (artículo 37 del RGPD):
  - El tratamiento de datos personales lo lleva a cabo una autoridad u organismo público
  - Las **actividades principales** del responsable / encargado del tratamiento consisten en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una **observación habitual y sistemática** de interesados **a gran escala**
  - Las actividades principales del responsable / encargado consiste en el tratamiento a gran escala de categorías especiales de datos personales (artículo 9 del RGPD) y de datos relativos a condenas e infracciones penales (artículo 10 del RGPD)

- ❑ También es obligatorio en aquellos supuestos previstos en el artículo 34.1 de la LOPDGDD
- ❑ Puede designarse de forma voluntaria

El delegado de protección de datos: ¿es obligatorio nombrarlo? (cont.)

- Las **actividades principales** del responsable / encargado del tratamiento consisten en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una **observación habitual y sistemática** de interesados **a gran escala**
- **Actividades principales**
  - ¿Cuál es la actividad principal del responsable / encargado del tratamiento?
  - ¿Es posible llevar a cabo esa actividad sin tratar datos personales?
- **A gran escala**
  - Tratamiento de datos de pacientes por un hospital
  - Tratamiento de datos de desplazamiento de las personas que utilizan el sistema de transporte público de una ciudad
  - Tratamiento de datos de geolocalización en tiempo real de clientes de una cadena internacional de comida con fines estadísticos
  - Tratamiento de datos de clientes por una compañía de seguros o un banco
- **Observación habitual y sistemática**
  - Operar una red de telecomunicaciones
  - Redireccionar correos electrónicos
  - Seguimiento de ubicación mediante aplicaciones móviles
  - Seguimiento de datos de bienestar, estado físico y salud mediante dispositivos móviles

- Supuestos del artículo 34.1 de la LOPDGDD
  - Los colegios profesionales y sus consejos generales
  - Los centros docentes, así como las Universidades públicas y privadas
  - Las entidades que exploten redes y presten servicios de comunicaciones electrónicas, cuando traten habitual y sistemáticamente datos personales a gran escala
  - Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de las personas usuarias del servicio
  - Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito
  - Los establecimientos financieros de crédito
  - Las entidades aseguradoras y reaseguradoras
  - Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores
  - Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural

El delegado de protección de datos: ¿es obligatorio nombrarlo? (cont.)

- Supuestos del artículo 34.1 de la LOPDGDD (cont.)
  - Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo
  - Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de las personas afectadas o realicen actividades que impliquen la elaboración de perfiles de las mismas
  - Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes (excepción: profesionales de la salud que ejerzan su actividad a título individual)
  - Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas
  - Las personas operadoras que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos
  - Las empresas de seguridad privada
  - Las federaciones deportivas, cuando traten datos de menores de edad

- En un futuro ...

  - Obligatoriedad de nombrar a un delegado de protección de datos en aquellas empresas que tengan más de 50 trabajadores (Anteproyecto de Ley por la que se transpone la Directiva de *Whistleblowing*)

El delegado de protección de datos: ¿debe comunicarse su nombramiento a la AEPD?

- Sí, siempre

  - En el plazo de 10 días desde su nombramiento
  - ¿Cómo hacerlo? **https://sedeagpd.gob.es/sede-electronica-web/vistas/formDelegadoProteccionDatos/procedimientoDelegadoProteccion.jsf**

Materiales

- Reglamento General de Protección de Datos: **https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32016R0679**
- Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales: **https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673**
- Ley de servicios de la sociedad de la información y de comercio electrónico: **https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758**
- Ley General de Telecomunicaciones: **https://www.boe.es/buscar/act.php?id=BOE-A-2014-4950**
- Directrices sobre los delegados de protección de datos (DPD), adoptadas el 13 de diciembre de 2016
- Preguntas frecuentes de la Agencia Española de Protección de Datos sobre la figura del delegado de protección de datos: **https://www.aepd.es/es/preguntas-frecuentes/4-responsable-encargado-y-dpd/1-delegado-de-proteccion-de-datos#:~:text=%C2%BFQu%C3%A9%20es%20un%20Delegado%20de,en%20el%20responsable%20o%20encargado.**

HERRAMIENTAS GRATUITAS DE LA AEPD PARA EL CUMPLIMIENTO EN MATERIA DE PROTECCIÓN DE DATOS

La Agencia Española de Protección de Datos (AEPD) proporciona una serie de herramientas gratuitas a las empresas que facilitan la comprensión y cumplimiento de aquellas obligaciones que la normativa de protección de datos, principalmente el Reglamento General de Protección de Datos (UE) 2016/279 (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), establecen para los responsables y encargados del tratamiento de datos personales. Estas herramientas se pueden encontrar en la página oficial de la AEPD en la sección de Guías y Herramientas > Herramientas.

HERRAMIENTAS GESTIÓN DEL RIESGO

En primer lugar, a lo largo del transcurso de nuestra primera sesión [8 de junio] abordaremos **las herramientas de la AEPD destinadas a facilitar la identificación y gestión de los riegos** que pueda conllevar el tratamiento de los datos personales que efectúa una empresa, así como ayudar a identificar las ocasiones donde resulte necesario elaborar una evaluación de impacto, y cómo hacerlo, y aquellas donde resulte necesario efectuar una consulta previa ante la AEPD.

Antes de proceder a explicar el funcionamiento de las herramientas de gestión del riesgo, debemos hacer un breve recordatorio de los artículos 35 y 36 del RGPD que desarrollan las obligaciones del responsable del tratamiento de los datos de realizar una evaluación de impacto (EIPD) y una consulta previa a la autoridad de control. El tratamiento de los datos personales puede generar un impacto adverso en las personas físicas afectadas por el mismo. Es por ello que el RGPD demanda al responsable del tratamiento, en virtud del principio de responsabilidad proactiva, la identificación, evaluación y mitigación realizadas de una forma objetiva, del riesgo para los derechos y libertades de las personas en los tratamientos de datos personales. La mitigación ha de realizarse mediante la adopción de medidas técnicas y organizativas que garanticen y, además, permitan demostrar la protección de dichos derechos.

Con carácter general, el RGPD no exige ningún requisito explícito a la hora de ejecutar la gestión del riesgo. En consecuencia, todas las empresas con independencia del tratamiento que lleven a cabo, deben identificar aquellos riesgos que se deriven de su tratamiento y buscar y aplicar medidas que permitan mitigar su impacto. No obstante, y para aquellos tratamientos que impliquen un alto riesgo, el RGPD sí establece unos requisitos mínimos que ha de tener su gestión. Estos se derivan, especialmente, de las obligaciones establecidas en los artículos 35 “Evaluación de impacto relativa a la protección de datos” (EIPD), y el artículo 36 “Consulta previa” del RGPD. La Evaluación de Impacto (EIPD) es una especificidad dentro de la gestión del riesgo. Mientras que, como hemos dicho previamente, la gestión del riesgo es obligatoria para todo tratamiento, las obligaciones concretas que se establecen para la EIPD son obligatorias, exclusivamente, para tratamientos de alto riesgo. La autoridad de control es la que establece con carácter general aquellos tratamientos que requieren de una evaluación de impacto, no obstante, podemos citar como ejemplo aquellos que implican un tratamiento automatizado como la elaboración de perfiles, aquellos que implican un tratamiento a gran escala de categorías especiales de datos, etc. Por otro lado, las consultas previas son aquellas consultas que se efectúan a la autoridad de control para buscar asesoramiento sobre las medidas mitigadoras a aplicar cuando, tras haber realizado una EIPD, el riesgo residual resultante es elevado y podría poner en riesgo los derechos y libertades de las personas físicas afectadas. Pues bien, para facilitar el cumplimiento de estas obligaciones, la AEPD pone a disposición de las empresas las siguientes herramientas:

1. FACILITA RGPD
2. FACILITA EMPRENDE

3. GESTIONA EIPD
4. EVALÚA RIESGO RGPD

Para conocer cuándo utilizar cada una de estas herramientas, dejamos a continuación un cuadro explicativo.

¿El tratamiento de datos personales conlleva un riesgo escaso o bajo?

- FACILITA RGPD: La herramienta permite a la empresa generar documentación para cumplir con los requisitos del RGPD cuando el tratamiento conlleva un riesgo bajo. Si la herramienta de FACILITA RGPD considera que no aplica a la empresa por ser el riesgo del tratamiento no escaso, la misma indica a la empresa la necesidad de llevar a cabo una gestión de riesgos.

¿La empresa que trata los datos personales es una empresa de nueva creación que aplica herramientas innovadoras o novedosas relacionadas con las nuevas tecnologías?

- FACILITA EMPRENDE: Es una herramienta que sirve de apoyo para caracterizar los tratamientos realizados por empresas con nuevas tecnologías y startups de reciente creación (que suelen ser de mayor dificultad en este tipo de empresas que utiliza tecnologías innovadoras). Este tipo de empresas al utilizar tecnologías muy innovadoras muchas veces implican un tratamiento de datos de alto riesgo por lo que en ocasiones esta herramienta te remite a GESTIONA EIPD para que evalúes el riesgo y veas si es necesario una EIPD.

¿Se desconoce el riesgo que implica el tratamiento de datos?

- GESTIONA EIPD: Esta herramienta es un asistente previo para preparar la gestión del riesgo para los derechos y libertades y permite a la empresa saber si resulta necesario que efectúe una evaluación de impacto en protección de datos.

¿El tratamiento de los datos personales conlleva un riesgo alto?

- EVALÚA- RIESGO RGPD: Esta herramienta permite a las empresas hacer una primera evaluación del riesgo intrínseco; establece la necesidad de realizar una Evaluación de Impacto y estima el riesgo residual si se utilizan medidas y garantías para mitigar los factores de riesgo específicos. Al estimar este riesgo residual te permite saber si resulta necesario que se efectúe una consulta previa a la AEPD.

HERRAMIENTA 1: FACILITA RGPD

¿En qué consiste la herramienta?

FACILITA RGPD es una herramienta de ayuda para las empresas que realicen un tratamiento de datos personales de escaso riesgo (e.g. tratamientos de datos de contacto y facturación de los clientes o proveedores de una pequeña empresa) para facilitarles la adaptación al cumplimiento del Reglamento General de Protección de Datos. **ES DE LAS HERRAMIENTAS MÁS UTILIZADAS POR LAS EMPRESAS.** En concreto, la herramienta permite, a través de tres pantallas de preguntas valorar la situación de la empresa en términos de tratamiento de los datos personales. En base a ello, FACILITA RGPD genera documentos de protección de datos adaptados a la empresa concreta, entre otros, cláusulas informativas que debe incluir en sus formularios de recogida de datos personales, el registro de actividades de tratamiento. El enlace para acceder a dicha herramienta es el siguiente: **https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQwMjAzNDkxNjUxNzUxOTk1NTgw?updated=true**.

Cuestiones a tener en consideración

- La mera obtención de los documentos NO SUPONE el cumplimiento automático de las obligaciones del RGPD y la LOPDGDD para los responsables y encargados de tratamiento, únicamente proporciona orientación y facilita la comprensión de dichas obligaciones.
- La herramienta NO PUEDE utilizarse para tratamientos de datos personales que entrañen un elevado riesgo para los derechos y libertades de las personas físicas como tratamientos masivos, generación y uso de perfiles, video vigilancia, etc.
- Los datos subidos o aportados a esta herramienta SE ELIMINAN tras finalizar su uso, por lo que la AEPD no conocerá la información aportada.
- La ayuda proporcionada es general, por lo que puede NO ADAPTARSE a las características concretas de todas las empresas.

Instrucciones para su uso

Accediendo al enlace que se ha aportado anteriormente, la herramienta FACILITA RGPD despliega un cuestionario o auto test que la empresa debe ir completando, marcando las respectivas casillas que resulten de aplicación a su caso concreto. Primero, la herramienta hace tres preguntas acerca del tratamiento de datos para asegurar que el tratamiento efectuado por la empresa no entraña un elevado riesgo para los derechos y libertades de las personas físicas. **[Ver las capturas de pantalla que se adjuntan en la presentación]** Si de la respuesta que se proporcione a las preguntas la herramienta entiende que no hay un riesgo alto para los derechos y libertades de las personas afectadas, la herramienta pasa a la segunda fase del cuestionario. Si no es el caso, la herramienta muestra un mensaje emergente señalando que la herramienta no es adecuada para el que la está utilizando y que debe realizar un análisis de riesgos. Si se supera la primera fase, la herramienta señala que es adecuada para el tratamiento y procede a recabar información de la empresa para generar los formularios correspondientes de protección de datos. "**Ha respondido de forma negativa a todas las cuestiones anteriores, por tanto, se podría entender que los tratamientos realizados por su entidad entrañan, a priori, un escaso nivel de riesgo para los derechos y libertades de los interesados y por tanto se encontraría en disposición de utilizar el siguiente programa."** Las preguntas que se formulan para generar los formularios hacen referencia a las siguientes cuestiones:

1. Datos identificativos de la empresa (nombre, dirección de correo electrónico, NIF, teléfono, etc.). Estos datos sirven para personalizar los documentos o formularios de protección de datos que emite la herramienta.
2. A continuación, la herramienta pregunta las categorías de interesados de los cuales se tratan los datos: (i) clientes personas físicas, (ii) empleados, (iii) candidatos, (iv) proveedores personas físicas. Si se responde afirmativamente a la categoría de interesado, la herramienta desplegará un cuestionario con preguntas acerca de los datos que se recaban de esas categorías de interesados (tipos de datos (bancarios, identificativos, etc.); para que finalidades los recaba (prestar servicio, etc.) y a quién entrega esos datos). **[Ver captura de pantalla ejemplificativa en la presentación]**

Asimismo, la herramienta también pregunta las siguientes cuestiones (las mismas se preguntas porque la comunicación de datos a terceros subcontratados o la recogida de imágenes con cámaras de video vigilancia puede conllevar un riesgo alto):

- ¿Su organización capta imágenes mediante cámaras de video vigilancia con fines de seguridad?
- ¿Su organización tiene contratadas terceras empresas que le prestan servicios como pueden ser los de mantenimiento de su página web, desarrollo de

programas informáticos, proveedor de correo electrónico, hosting, servicio de limpieza, servicio de video vigilancia u otros?

Una vez respondido el cuestionario, la herramienta generará los documentos de protección de datos adaptados a la empresa. Estos documentos se descargarán en formato Word que podrá ser editado por la empresa a su discreción para adaptar y personalizar en mayor medida el tratamiento de los datos que realiza.

REMINDER: La mera obtención de los documentos NO SUPONE el cumplimiento automático de las obligaciones del RGPD y la LOPDGG.

HERRAMIENTA 2: FACILITA EMPRENDE

¿En qué consiste la herramienta?
Esta herramienta busca dar apoyo a personas emprendedoras y startups (menos de 10 años de creación) cuyos tratamientos se caracterizan por un fuerte componente innovador, con empleo de tecnologías emergentes. En concreto, la herramienta permite caracterizar los tipos de tratamientos realizados y proporcionar los documentos que se enumeran a continuación y que dan apoyo a la empresa para cumplir con las obligaciones de protección de datos:

1º) Una política de información en dos niveles compuesta por las cláusulas de informativas a proporcionar en el momento de la recogida de datos y una política de privacidad.
2º) El Registro de Actividades de Tratamiento (RAT) pre cumplimentado.
3º) El modelo de hoja de registro de incidentes para cumplir con el artículo 33.5 relativo a la documentación de las brechas de seguridad que afecten o puedan afectar a datos personales.
4º) Un conjunto de cláusulas contractuales a incluir en los contratos que suscriba con las personas encargadas de tratamientos de datos y proveedores.
5º) Si su empresa cuenta con una página web que utiliza cookies y tecnologías similares, una política de cookies.
6º) Un conjunto de directrices y recomendaciones, para ayudarle en el proceso de adecuación, en relación con la gestión de brechas de seguridad, la atención al ejercicio de los derechos, recomendaciones sobre video vigilancia, indicaciones específicas con relación a la gestión de los riesgos de sus tratamientos, así como a las estrategias de privacidad y medidas de seguridad que deberá implementar.
7º) Una relación de recomendaciones para prevenir el acoso digital.

El enlace para acceder a esta herramienta es el siguiente: **https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQwMjY4MzAxNjUxOTI3NzM2MjM5?updated=true.**

Cuestiones a tener en consideración
- La mera obtención de los documentos NO SUPONE el cumplimiento automático de las obligaciones del RGPD y la LOPDGDD.
- Cabe la posibilidad de por los tipos de tratamiento que suelen ir asociados a los modelos de negocios de emprendedores y startups, la empresa no tenga un riesgo bajo para los derechos y libertades de las personas físicas y entonces, tenga que personalizar y complementar los entregables facilitados por esta herramienta.
- La información SE ELIMINA terminada la sesión por lo que la AEPD no puede conocer ni tratar dicha información.

Instrucciones para su uso
Accediendo al enlace que se ha aportado anteriormente, la herramienta FACILITA EMPRENDE despliega un cuestionario o auto test que la empresa debe ir

completando, marcando las respectivas casillas que resulten de aplicación a su caso concreto. El proceso de cumplimentación está estructurado en tres partes:

En primer lugar, se evalúa si la empresa encuadra en el perfil de una startup tecnológica, identificando las tecnologías utilizadas (e.g. plataformas colaborativas, aplicaciones móviles, etc.) y recogiendo los datos para generar el documento personalizado (i.e. nombre de la empresa, NIF, descripción de la actividad etc.). **[Ver las capturas de pantalla que se adjuntan a la presentación]**

Una vez recogidos estos datos, la herramienta pregunta en calidad de qué se está tratando datos personales: (i) responsable; (ii) encargado; (iii) desarrollador. Identificado el rol, la herramienta pasa a solicitar información sobre aquellos tratamientos de tipo básico que la empresa puede estar gestionando como responsable (datos de clientes potenciales, clientes, empleados, candidatos, proveedores personas físicas y qué datos en concreto o para qué finalidad) así como los datos de identificación de aquellas terceras partes que le estén prestando un servicio a su entidad. A partir de esta información la herramienta generará información de utilidad para ayudar a la empresa en el cumplimiento de sus obligaciones: elaboración de los registros de actividades de tratamiento, cláusulas informativas, modelos de contratos con encargados de tratamiento, etc.

Asimismo, la herramienta también pregunta las siguientes cuestiones (las mismas se preguntas porque la comunicación de datos a terceros subcontratados o la recogida de imágenes con cámaras de video vigilancia puede conllevar un riesgo alto):

- ¿Su startup capta imágenes mediante cámaras de video vigilancia con fines de seguridad?
- ¿Su startup dispone de empresas contratadas que le prestan servicios como por ejemplo los de mantenimiento o alojamiento web, desarrollo de software, servicios de correo electrónico, servicio de limpieza, video vigilancia, etc.?

[Si estas preguntas se responden afirmativamente la herramienta te solicita datos relacionados con ellas].

Finalizadas estas secciones anteriores, existe una tercera fase que es variable en función de la información previamente aportada. En concreto, se analizan aquellas actividades de tratamiento que se soportan sobre las tecnologías empleadas por la empresa, caracterizando, para cada una de ellas, el nivel de riesgo que representan. A partir del análisis de los datos, las finalidades y los factores de riesgo que incorporan la herramienta realiza una recomendación respecto a la aproximación a la gestión del riesgo que debería seguir la empresa. Como resultado final, la herramienta de FACILITA EMPRENDE te facilita:

- El saber si procede o no realizar una gestión del riesgo y una evaluación de impacto por ser el tratamiento de los datos que lleva a cabo la empresa tecnológica de alto riesgo.
- Un documento base adaptado a los tratamientos que realiza la empresa (cláusulas de firmantes, cartel de video vigilancia, etc.) y señalando aquellas cuestiones necesarias para que cumpla con la adaptación a la normativa de protección de datos. Este documento es una versión de mínimos y deberá ser validado por el responsable. El documento se descarga en formato Word, pudiendo ser editado por la empresa a su gusto.

HERRAMIENTA 3: GESTIONA EIPD

¿En qué consiste la herramienta?
Es una herramienta que funciona como asistente previo (i.e. aspectos básicos a tener en cuenta) para proporcionar ayuda en la elaboración de una evaluación de impacto (EIPD o PIA), la cual se debe llevar a cabo para ver los riesgos que suponen ciertos tratamientos de datos en los derechos y libertades de las personas físicas (no siempre se requiere una EIPD); o una gestión de los riesgos. La herramienta está destinada para los pequeños y medianos responsables (PYMES) del tratamiento de datos personales que no dispongan en su organización de un marco para la gestión del riesgo. En concreto, GESTIONA EIPD es como una especie de una lista cerrada de elementos a tener en cuenta, y aporta a las personas responsables las bases mínimas para iniciar las actividades de análisis y gestión de riesgos en el ámbito del RGPD, incluyendo requisitos de cumplimiento normativo y medidas encaminadas a reducir o mitigar el riesgo del tratamiento. El enlace para acceder a esta herramienta es el siguiente: **https://gestiona.aepd.es/.**

Cuestiones a tener en consideración
- La mera obtención de los documentos NO SUPONE el cumplimiento automático de las obligaciones del RGPD y la LOPDGDD para los responsables y encargados de tratamiento, únicamente proporciona orientación y facilita la comprensión.
- La herramienta NO SUPONE la realización de una evaluación de impacto, sino que sirve como punto de partida. En concreto, el empleo de esta herramienta se debe realizar teniendo en consideración la Guía de Gestión de riesgo y evaluación de impacto en tratamientos de datos personales de la AEPD, la lista de verificación para determinar la adecuación formal de una EIPD y la presentación de consulta previa.
- Esta herramienta NO PUEDE ENTENDERSE como una forma de aplicar las medidas técnicas y organizativas de seguridad incluidas en el artículo 32 del RGPD.
- Esta herramienta se utiliza en conjunción con el listado de tratamientos de datos personales en los que es obligatorio hacer una EIPD: **https://www.aepd.es/es/documento/listas-dpia-es-35-4_0.pdf**.
- Los datos que se señalen e incluyan en el cuestionario de GESTIONA EIPD se guardarán de forma local en el ordenador. Ello permite iniciar la gestión de riesgos y cerrar la sesión y luego volver a donde lo dejaste metiendo el nombre que has decidido darle al análisis. Para ello hay que pinchar al inicio de la herramienta en la opción señalada como “CARGAR ANÁLISIS PREVIOS”.

Instrucciones para su uso
Accediendo al enlace que se ha aportado anteriormente, la herramienta GESTIONA EIPD despliega un cuestionario o auto test que la empresa debe ir completando, marcando las respectivas casillas que resulten de aplicación a su caso concreto. En primer lugar, para iniciar sesión la herramienta te solicita que elijas entre iniciar una EIPD o una gestión de los riesgos. Una vez seleccionas un nombre denominar a la EIPD o para la gestión de riesgos comienza el análisis.

OPCIÓN EIPD:
Si seleccionas EIPD, se formulan ocho preguntas sobre los siguientes temas:
(i) el tipo de tratamientos que lleva a cabo tu empresa se incluye entre aquellos que la AEPD considera que requieren una EIPD;
(ii) si se van a tratar categorías especiales de datos;
(iii) finalidades del tratamiento (menores de edad, hacer perfiles, datos a gran escala de zonas de acceso público, etc.);
(iv) tecnologías empleadas para el tratamiento;

(v) existencia de encargados de tratamiento, cesiones o transferencias internacionales de datos;
(vi) percepción del riesgo por el responsable del tratamiento y por el delegado de protección de datos (DPO) y;
(vii) base jurídica del tratamiento.

Las preguntas anteriores sirven para determinar el riesgo que entraña el tratamiento de los datos y si se precisa hacer una evaluación de impacto. Una vez se responden las preguntas anteriores, se inicia una nueva fase que consta de las siguientes secciones:

- Ciclo de vida de los datos
- Análisis de la necesidad y proporcionalidad del tratamiento
- Identificación de los riesgos
- Gestión de los riesgos

Las mismas son comunes al proceso de gestión de los riesgos por lo que las desarrollaremos una única vez, para el proceso de gestión de los riesgos. Tras haber incluido la información que precisaban los campos anteriores, la herramienta genera un resultado que puede ser “ACEPTABLE” o “NO ACEPTABLE”. Asimismo, te da la opción de generar un informe de riesgos para continuar con la EIPD o un informe para seguir identificando los riesgos y salvaguardas del tratamiento.

OPCIÓN GESTIÓN DEL RIESGO:
Si seleccionas la opción de gestión de riesgos, la herramienta inicia un cuestionario con preguntas. En primer lugar, la herramienta recoge información sobre el ciclo de vida de los datos. En concreto, información sobre (i) el proceso de captura de los datos; (ii) la clasificación y almacenamiento de los datos; (iii) el uso y tratamiento de los datos; (iv) la cesión o transferencia de los datos a un tercero para su tratamiento; y (v) la destrucción de los datos. **[A modo ejemplificativo se muestra en la presentación capturas de pantalla de esta primera fase de ciclo de los datos.]** Para cada de estas categorías se deben rellenar cuatro campos: actividades; categorías de datos; intervinientes y tecnologías aplicadas. Una vez completada esta primera fase, la herramienta procede a identificar los riesgos y amenazas. Seleccionadas las amenazas, la herramienta mostrará las amenazas seleccionadas con las posibles medidas de control asociadas a cada una de ellas. La empresa debe seleccionar aquellas medidas que sean necesarias para mitigar el riesgo de la amenaza. Además, deberá seleccionar la probabilidad y el impacto de que ocurra dicha amenaza. Después de seleccionar las medidas de control, se debe evaluar la probabilidad y el impacto calculando nuevamente el riesgo residual. Este proceso es necesario realizarlo para cada una de las amenazas seleccionadas. Cuando se hayan rellenado todas las medidas de control, probabilidades e impactos de las amenazas, la herramienta generará un resultado que puede ser “ACEPTABLE” o “NO ACEPTABLE” que, en última instancia, deberá ser validado por el responsable.Asimismo, la herramienta te da la opción de generar un informe de riesgos con el resultado del análisis o un informe final con el que iniciar la identificación y gestión de los riesgos para los derechos y libertades de los interesados con el objeto de diseñar el plan de acción con las medidas de control. Todo ello en formato Excel o pdf.

<u>HERRAMIENTA 4: EVALÚA- RIESGO RGPD</u>

¿En qué consiste la herramienta?
Es una herramienta para el análisis de necesidad de una Evaluación de Impacto en Protección de Datos.

La misma tiene un triple objetivo: (i) hace una primera evaluación del riesgo intrínseco; (ii) establece la necesidad de realizar una Evaluación de Impacto y (iii) estima el riesgo residual si se utilizan medidas y garantías para mitigar los factores de riesgo específicos. El enlace para acceder a esta herramienta es el siguiente:
https://www.aepd.es/es/herramienta/EvaluaRiesgo_RGPD.zip.

Cuestiones a tener en consideración

- A diferencia de las herramientas anteriores que se pueden usar en línea, esta herramienta precisa de su descarga para poder ser empleada. La misma se descarga en formato Zip, que contiene el Excel donde se lleva a cabo el proceso.
- Los factores de riesgo desplegados en esta herramienta NO tienen carácter exhaustivo. Esto quiere decir que cada empresa como responsable del tratamiento deberá identificar los aspectos específicos que le afectan en su actividad particular, en el procesamiento de datos personales que requiera el despliegue de su negocio y, previo asesoramiento, incluirlo en su evaluación.
- Esta herramienta se complementa con la GUÍA DE GESTIÓN DEL RIESGO Y EVALUACIÓN DE IMPACTO EN TRATAMIENTOS DE DATOS PERSONALES que unifica los criterios e interpretaciones de las autoridades en materia de protección de datos.
  El enlace de acceso a esta guía es el siguiente:
  https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

  Esta guía permite un conocimiento más profundo de la gestión de los riesgos y es aplicable a cualquier tratamiento con independencia del nivel de riesgo. La misma se estructura en tres apartados: el primero contiene una descripción de los fundamentos de la gestión de riesgos para los derechos y libertades; el segundo incluye un desarrollo metodológico básico para la aplicación de la gestión del riesgo, y el último está enfocado en los casos en los sea preciso realizar una EIPD, con las orientaciones necesarias para llevarla a cabo.
  A continuación, se adjunta una pequeña tabla con algunos de los puntos clave de esta guía.

- Se especifica que la gestión del riesgo no puede, en ningún caso, sustituirse por el cumplimento normativo, o por una póliza de seguros que cubra la responsabilidad de la organización en caso de que haya una infracción de la normativa de protección de datos, sino que, ante cualquier tratamiento, la organización tiene adoptar medidas técnicas y organizativas que protejan los derechos y libertades de las personas. - Se destaca la importancia que tiene la gestión de la seguridad de la información. En concreto se indica que la implementación en la organización de modelos de gestión, como el Sistema de Gestión de la Seguridad de la Información (SGSI) y de directrices como las normas ISO 27000 o el Esquema Nacional de Seguridad, además de políticas de información de la entidad y las políticas de seguridad, son medios para poder gestionar los riesgos de forma efectiva y eficaz. No obstante, la implementación de estos modelos no es suficiente, sino que las medidas de seguridad que se implementen en la organización tienen que revisarse continuamente dado que la actividad de tratamiento, y por ende el riesgo, puede evolucionar por diversos factores. - Se incluye el concepto de “Gobernanza de los riesgos para los derechos y libertades” relacionado con el cumplimiento del principio de responsabilidad proactiva, y que indica que en la organización se deben

implementar políticas de protección de datos efectivas, prácticas y ejecutivas, no limitadas a una mera declaración de voluntad de compromiso.
- Se introducen se introducen dos nuevos conceptos para el cálculo del nivel del riesgo cuando hay dos o más factores de riesgo que apunten a un determinado nivel de impacto, y cuando haya dos o más indicios que apunten a un determinado nivel de probabilidad: el coeficiente de impacto acumulado y el coeficiente de probabilidad acumulado.
- Se desarrolla la exigencia relativa a la evaluación de la necesidad y proporcionalidad del tratamiento, haciendo una ponderación del juicio de proporcionalidad, del juicio de necesidad y del juicio de proporcionalidad en sentido estricto.

Instrucciones para su uso

En primer lugar, la empresa debe descargarse la herramienta en formato ZIP y abrir el Excel que se contiene en la misma, pues como hemos dicho anteriormente, esta herramienta no puede ser utilizada en línea como las demás. Una vez descargada, la herramienta despliega un cuestionario o auto test que la empresa debe ir completando, marcando las respectivas casillas que resulten de aplicación a su caso concreto.En concreto, a través de once pestañas diferentes, EVALÚA – RIESGO RGPD muestra aquellos factores de riesgo que pueden afectar al tratamiento de los datos personales. La empresa, haciendo un recorrido secuencial a través de las once pestañas deberá determinar la aplicabilidad de cada factor de riesgo. Seleccionando el cuadro de aplicabilidad de cada factor de riesgo se desplegarán en muchos casos ejemplos, además de permitir seleccionar “APLICA” o “NO APLICA”. Asimismo, a lado de la categoría de factor de riesgo, se añade una segunda columna que indica “MITIGACIÓN” de forma que en función de las medidas y garantías con las que cuente la empresa para mitigar dichos factores de riesgo se indique una de las cuatro categorías siguientes: (1) no mitigado; (2) limitadamente mitigado; (3) significativamente mitigado; (4) mitigado.

Las once pestañas que contiene el Excel son las siguientes:

(i) finalidades del tratamiento (si se lleva a cabo un perfilado, un rastreo de contactos, decisiones automatizadas, localización, etc.);
(ii) tipos de datos utilizados (datos biométricos, datos genéticos, metadatos, datos sanitarios, datos relativos a condenas, etc.);
(iii) extensión y alcance del tratamiento (es un tratamiento exhaustivo, el volumen de datos es elevado, es un tratamiento a gran escala, etc.);
(iv) categorías de interesados que se tratan (discapacitados, colectivos vulnerables, menores de 14 años, personas con enfermedades mentales, etc.);
(v) factores técnicos empleados en el tratamiento (servicios web, aplicaciones móviles, video vigilancia, reconocimiento facial, etc.);
(vi) recogida y generación de los datos tratados (acceso a bases de datos sobre fraude, datos personales obtenidos en zonas de acceso público, combinación de conjuntos de datos, etc.);
(vii) efectos colaterales del tratamiento de los datos (podría determinar la situación financiera, puede provocar o genera discriminación, posible daño reputacional, etc.);
(viii) el sector donde opera el responsable o encargado (empresa de biotecnología, entidad financiera, hospitales, etc.);
(ix) comunicaciones de los datos (difusión indiscriminada de identificadores únicos, transferencia a países sin un nivel adecuado de protección, etc.);
(x) otros factores (este campo es para que rellene la empresa con aquellos otros factores de riesgo que considere que apliquen y que no se encuadren en las categorías anteriores);

(xi) seguridad en el tratamiento de los datos (pérdida de trazabilidad, fallos en medidas y garantías técnicas de protección, pérdida de integridad, etc.)

[Dejamos en la presentación capturas de pantalla mostrando algunas de las diferentes once pestañas sobre factores de riesgo.]

Las categorías anteriormente enunciadas contienen aquellas categorías de datos, alcances de tratamiento, finalidades del tratamiento, etc. que implican un elevado nivel de riesgo, de forma que, si aplican, normalmente la empresa llevará a cabo un tratamiento de los datos de alto riesgo. Una vez se hayan completado todos los campos con los factores de riesgo y el nivel de protección que tiene la empresa para mitigar esos factores, la herramienta te ofrece un resultado donde se indica el nivel de riesgo intrínseco y se valora la necesidad de que la empresa realice una evaluación de impacto.

- Si el riesgo intrínseco es alto, significa que, en principio, deberá llevarse a cabo una evaluación de impacto.
- Si el riesgo residual es alto, significa que, en principio, deberá efectuarse una consulta previa ante la autoridad de control.

No obstante, la decisión final debe ser valorada por el responsable del tratamiento, que es quien tiene conocimiento pleno del caso. En concreto, en la pestaña de resultados la herramienta te indica la valoración del riesgo intrínseco y del riesgo residual, señalando si el riesgo es alto o bajo. Asimismo, la empresa tiene la opción de generar un informe con los resultados, así como de obtener una lista de fuentes de riesgo por categorías.

En segundo lugar, a lo largo del transcurso de nuestra segunda sesión [23 de junio] abordaremos las herramientas de la AEPD destinadas a la identificación de aquellas brechas de seguridad que, por su carácter, requieran ser comunicadas a las personas físicas aceptadas; así como el canal de consultas de la AEPD destinado a los delegados de protección de datos, que actúan como intermediarios entre las empresas y las autoridades de control en materia de protección de datos.

HERRAMIENTA BRECHA DE SEGURIDAD

Antes de proceder a explicar el funcionamiento de la herramienta de comunicación de la brecha de seguridad, debemos hacer un breve recordatorio de los artículos 33 y 34 del RGPD que desarrollan las obligaciones del responsable del tratamiento de los datos de comunicar a la autoridad de control competente y a las personas físicas afectadas, aquellas brechas de seguridad que constituyan un riesgo alto para los derechos y las libertades de las personas físicas. Una brecha de datos personales es un incidente de seguridad que ocasiona la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos.Una brecha de datos personales puede tener efectos adversos sobre las personas físicas titulares de los datos afectados, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas. El artículo 33 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas. El responsable de tratamiento debe valorar el nivel de riesgo de una brecha de datos personales y notificarla a la autoridad de control cuando exista tal riesgo, y además cuando el riesgo sea alto el responsable también deberá comunicar la brecha a las personas afectadas conforme al artículo 34 del RGPD.

Esta comunicación con carácter general, deberá contener los siguientes requisitos:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Para ayudar en la toma de esta decisión la AEPD pone a disposición de las empresas la herramienta COMUNICA BRECHA, la cual ayuda a determinar si se debe notificar a las personas físicas por la brecha de seguridad.

HERRAMIENTA: COMUNICA BRECHA

¿En qué consiste la herramienta?
Es una herramienta que permite a la empresa valorar la obligación de informar a las personas físicas afectadas por una brecha de seguridad de los datos personales (artículo 34 RGPD), pues una brecha de seguridad que ponga en riesgo la integridad de los datos puede suponer una imposición de sanciones económicas por la AEPD. Sirve de ayuda principalmente a las PYMES y autónomos para saber cómo actuar en caso de sufrir una brecha de seguridad. La herramienta tiene un formato de auto test y está destinada al responsable de protección de datos para que sepa si tiene que notificar o no la brecha en función de la importancia, el tipo de datos afectados y la gravedad del incidente.Una vez recopilada la información, la herramienta emite un informe, incluyendo las posibles acciones a realizar. Asimismo, la herramienta emitirá una de las tres respuestas:

- Es necesario informar de la brecha de seguridad a las personas afectadas.
- No es necesario informar de la brecha de seguridad, pues se considera que la información expuesta no afecta de forma relevante a las personas físicas.
- La información suministrada no es suficiente para determinar el riesgo.

El enlace para acceder a esta herramienta es el siguiente: **https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQwMjY4MzExNjUxOTI3ODQ1NDg3?updated=true.**

Cuestiones a tener en consideración

- La mera obtención de los documentos NO SUPONE el cumplimiento automático de las obligaciones del RGPD y la LOPDGDD para los responsables y encargados de tratamiento, únicamente proporciona orientación y facilita la comprensión de dichas obligaciones.
- Los datos subidos o aportados a esta herramienta SE ELIMINAN tras finalizar su uso, por lo que la AEPD no conocerá la información aportada.
- Esta herramienta ayuda a la toma de decisiones, pero es responsabilidad última del responsable del tratamiento ver si corresponde notificar la brecha de seguridad.

Instrucciones para su uso
Accediendo al enlace que se ha aportado anteriormente, la herramienta COMUNICA BRECHA despliega un cuestionario o auto test que la empresa debe ir completando, marcando las respectivas casillas que resulten de aplicación a su caso concreto. En

primer lugar, la herramienta te pedirá que selecciones el sector de actividad al que se dedica la empresa de entre 10 opciones (e.g. telecomunicaciones, solvencia patrimonial, publicidad, entidades bancarias, etc.) y 1 categoría adicional para el caso de que la empresa identifiques con ninguna de las categorías anteriores. En segundo lugar, la empresa deberá facilitar los detalles sobre el incidente o la brecha de seguridad, facilitando información cómo, por ejemplo, si el incidente ha sido accidental o intencionado; cuál ha sido el origen del incidente; si ha sido o no un ciberincidente. Posteriormente, la empresa debe facilitar las consecuencias de dicho incidente y en qué grado podrían afectar las consecuencias identificadas a las personas físicas afectadas, indicando el nivel de gravedad que en su opinión merezca el incidente. A continuación, la empresa deberá introducir los tipos de datos que se han visto afectados y las personas afectadas, con especial referencia a si hay colectivos vulnerables como menores de edad, o si se trata de un número amplio de personas afectadas. Asimismo, la empresa deberá facilitar información temporal sobre la brecha, señalando la fecha en que se detectó el incidente con certeza y la fecha en que se inició la brecha de seguridad. Toda la información anterior sirve para determinar el nivel de riesgo de la brecha, pues sólo un nivel alto de riesgo para los derechos y libertades de las personas físicas afectadas implica la necesidad de notificarles la brecha de seguridad. En último lugar, la herramienta proporciona un resultado, señalando si de acuerdo a los datos facilitados procede o no comunicar la brecha de seguridad a las personas físicas afectadas.

HERRAMIENTA CANAL DE CONSULTAS DELEGADO DE PROTECCIÓN DE DATOS

Antes de proceder a explicar el funcionamiento del canal de consultas del delegado de protección de datos, debemos hacer un breve recordatorio de los artículos 37 y 39 del RGPD que desarrollan la figura del delegado de protección de datos, cuándo debe ser designado el mismo y las funciones que se le atribuyen. Para cumplir con la normativa de protección de datos y disponer de un intermediario entre las empresas que tratan los datos personales de las personas físicas y las autoridades de control en materia de protección de datos, el RGPD establece en su artículo 37 la designación de un delegado de protección de datos (DPD o DPO).Este nombramiento resulta obligatorio en ciertas ocasiones (el tratamiento de datos es por un organismo público, hay un tratamiento a gran escala de categorías especiales de datos, etc.) que vienen recogidos en los artículos 37 del RGPD y 34 de la LOPDGDD, y que coinciden con aquellas que suelen entrañar un riesgo para los derechos y libertades de los titulares de los datos. Estos DPD deben ser comunicados a través de la sede electrónica a la AEPD. Asimismo, y para el cumplimiento de sus funciones establecidas en el artículo 39 del RGPD (e.g. informar de sus obligaciones al responsable y encargado de tratamiento, cooperar con la autoridad de control, actuar como punto de contacto con la autoridad de control, etc.), la AEPD pone a disposición de los DPD de las empresas, el CANAL DE DPO para que los mismos puedan formular aquellas consultas que sean necesarias a la autoridad de control de los datos.

HERRAMIENTA: CANAL DEL DPD

¿En qué consiste la herramienta?
Esta herramienta tiene como finalidad atender las consultas planteadas ante la AEPD por las personas DPD, tanto del sector público como del privado, al desempeñar las funciones encomendadas en el artículo 39 del RGPD.Podrán plantear las consultas utilizando este canal:

1. Los DPD designados por las personas responsables y encargadas del tratamiento que hayan sido comunicados a la AEPD. La inclusión en la relación de DPD será suficiente para acreditar la designación.

2. Las organizaciones y asociaciones representativas de personas responsables y encargadas del tratamiento que ofrezcan a sus miembros los servicios de DPD.

Asimismo, existen una serie de requisitos que deben cumplirse para poder utilizar el CANAL DEL DPD:

- Identificarse como DPD, bien con un certificado electrónico, un certificado Clave PIN o una clave permanente. Las consultas anónimas no están permitidas en este canal.
- Facilitar toda aquella información que resulte necesaria sobre la cuestión o consulta que se plantea a la AEPD.
- El análisis que haya desarrollado previamente en el ejercicio de sus funciones como DPD.

El enlace para acceder a esta herramienta es el siguiente: **https://www.aepd.es/es/guias-y-herramientas/herramientas/canalDPD**

Cuestiones a tener en consideración

Este canal no podrá ser empleado para:

1. Cuestiones planteadas desde un punto de vista hipotético.
2. Cuestiones que pudiesen estar relacionadas con procedimientos que esté tramitando la AEPD, incluidas las relativas al estado de tramitación.
3. Cuestiones que pretendan la validación de documentos elaborados por responsables y encargados en materia de protección de datos, cuya responsabilidad recae sobre ellos en virtud del principio de responsabilidad proactiva.
4. Solicitudes de acceso a la información pública.
5. Consultas que se hayan presentado por el Canal de la Ciudadanía.
6. Consultas que se refieran a cuestiones que se encuentran ya explicadas y son accesibles en los materiales publicados en la página web de la AEPD, tales como las Guías, Preguntas Frecuentes y Herramientas elaboradas para facilitar el cumplimiento del RGPD.

Instrucciones para su uso

Accediendo al enlace que se ha aportado anteriormente, la empresa accederá a la herramienta. Una vez en ella, deberá seleccionar “SEDE ELECTRÓNICA” > CANAL DEL DPD y se le solicitará un certificado clave pin, un certificado electrónico o una clave permanente a través de la cual el DPD podrá acceder.

REMINDER: este canal solo puede ser utilizado por DPD previamente comunicados y registrados en la AEPD.

Una vez se haya accedido se podrá formular la consulta, la cual será respondida por la AEPD atendiendo a cuestiones de eficiencia y optimización de recursos, lo que puede repercutir en el tiempo de respuesta o la forma en que se responda. Asimismo, y debido a ello, se recomienda consultar antes las PREGUNTAS FRECUENTES que ya contienen muchas de las respuestas a las preguntas más habituales que se suelen formular en materia de protección de datos: **https://www.aepd.es/es/preguntas-frecuentes.** Estas preguntas frecuentes además se encuentran categorizadas por temas: video vigilancia, publicidad no deseada, tus derechos, etc.

Andrea Sánchez. Pérez-Llorca.

HERRAMIENTA 1: FACILITA RGPD

PASOS

A continuación os mostramos unas capturas de pantalla que muestran el funcionamiento de la herramienta FACILITA RGPD.

1º) Primero, la herramienta hace 3 preguntas acerca del tratamiento de datos para asegurar que el tratamiento efectuado por la empresa que la está utilizando la herramienta no entraña un elevado riesgo para los derechos y libertades de las personas físicas (ver capturas de pantalla). Si de la respuesta que se proporcione a las preguntas la herramienta entiende que no hay alto riesgo, la herramienta pasa a la segunda fase. Si no es el caso, la herramienta muestra un mensaje emergente señalando que la herramienta no es adecuada para el que la está utilizando.

aepd agencia española protección datos

RGPD HERRAMIENTA PARA TRATAMIENTOS DE ESCASO RIESGO ACILITA 2.0

Si la actividad de su organización pertenece a alguno de estos sectores, márquelo:

- ☐ Sanidad
- ☐ Solvencia patrimonial y crédito
- ☐ Generación y uso de perfiles
- ☐ Actividades políticas, sindicales o religiosas
- ☐ Servicios de telecomunicaciones
- ☐ Seguros
- ☐ Entidades bancarias y financieras
- ☐ Actividades de servicios sociales
- ☐ Publicidad
- ☐ Videovigilancia masiva (Videovigilancia de grandes infraestructuras como estaciones de ferrocarril o centros comerciales)
- ○ Ninguno de los anteriores

Si su organización trata alguno de los datos de la lista, márquelos:

- ☐ Datos que revelen origen étnico o racial
- ☐ Datos de opiniones políticas o religión
- ☐ Datos de afiliación sindical (excepto cuotas sindicales)
- ☐ Datos genéticos
- ☐ Datos biométricos dirigidos a identificar de manera unívoca a una persona
- ☐ Datos de salud física o mental
- ☐ Datos relativos a la vida sexual o a la orientación sexual
- ☐ Datos relativos a condenas o infracciones penales
- ☐ Geolocalización
- ○ Ninguno de los anteriores

Si su organización realiza alguno de los siguientes tratamientos, márquelo:

- ☐ Hacer o analizar perfiles
- ☐ Hacer publicidad y prospección comercial masiva a potenciales clientes
- ☐ Prestación de servicios de explotación de redes públicas o servicios de comunicación electrónica (proveedor de servicios de internet (LGT))
- ☐ Gestionar los asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical
- ☐ Gestión, control sanitario o venta de medicamentos
- ☐ Historial clínico o sanitario
- ○ Ninguna de las anteriores

Con los datos que ha proporcionado este programa no es adecuado para usted, ya que su empresa no cumple con los requisitos para seguir. Debe realizar un análisis de riesgos.

HERRAMIENTA 1: FACILITA RGPD

PASOS

2º) Si se supera la primera fase, la herramienta señala que es adecuada para el tratamiento y procede a recabar información de la empresa para generar los formularios correspondientes de protección de datos. Las preguntas que se formulan para generar los formularios hacen referencia a si se tratan datos de clientes, o de empleados; qué tipo de datos personales se tratan (identificativos, bancarios, etc.)

Ha respondido de forma negativa a todas las cuestiones anteriores, por tanto, se podría entender que los tratamientos realizados por su entidad entrañan, a priori, un escaso nivel de riesgo para los derechos y libertades de los interesados y por tanto se encontraría en disposición de utilizar el siguiente programa.

¿Su organización trata datos personales de clientes (personas físicas)?

Se refiere a datos personales de aquellas personas con las que usted mantiene una relación comercial.

○ Sí ○ No

¿Su organización trata datos personales de clientes (personas físicas)?

Se refiere a datos personales de aquellas personas con las que usted mantiene una relación comercial.

◉ Sí ○ No

A continuación marque qué datos personales trata de sus clientes

- ☐ Identificación (nombre, apellidos, NIF, dirección postal, teléfono, email)
- ☐ Características personales (estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad)
- ☐ Datos académicos
- ☐ Datos bancarios

Marque para qué utiliza los datos personales que solicita a sus clientes

- ☐ Prestarles un servicio
- ☐ Facturar
- ☐ Enviar publicidad postal o por correo electrónico
- ☐ Servicio postventa y fidelización

Marque a quien entrega los datos personales de sus clientes

Cumplimiento de obligaciones legales:

- ☐ Agencia Estatal de Administración Tributaria
- ☐ Instituto Nacional de la Seguridad social
- ☐ Bancos y entidades financieras
- ☐ Fuerzas y Cuerpos de Seguridad
- ☐ Otros

Otros:

- ☐ Gestoría

Los datos que incorpore en el programa desde esta pantalla hasta la finalización del programa, se van a utilizar para elaborar los documentos que se generan automáticamente adaptados a su organización

Nombre de la empresa

Dirección completa de la empresa

N.I.F.:

Teléfono

Dirección de correo electrónico:

Descripción de la actividad

HERRAMIENTA 1: FACILITA RGPD

PASOS

3º)Una vez contestadas las preguntas anteriores, la herramienta generará los documentos adaptados a los datos de la empresa y que previamente han sido comunicados a través de las preguntas anteriores. Los documentos se descargarán en formato Word, y podrá ser editado por la empresa a su gusto.

ESTA HERRAMIENTA ES DE LAS MÁS UTILIZADAS POR LAS EMPRESAS PYMES.

El programa ha terminado, cuando pulse el botón de FINALIZAR se generaran diversos documentos en formato editable.

RECUERDE, aunque se le ofrecen los documentos mínimos indispensables para estar en disposición de cumplir con el Reglamento de Protección de Datos, usted también debe realizar las siguientes acciones:

1. Incluir las cláusulas informativas en los formularios de solicitud de información, bien si utiliza formularios en papel o a través de su página web.
2. Implantar las medidas técnicas y organizativas que se le indican en el documento correspondiente.
3. Revisar los contratos que dispone actualmente e incluir las cláusulas contractuales y firmarlas en la última hoja.
4. Elaborar aquellos contratos que todavía no tiene e igualmente incluir las cláusulas contractuales y firmarlas en la última hoja.
5. Custodiar y mantener actualizados todos los documentos.
6. No olvide que no debe enviar nada a la Agencia Española de Protección de Datos, tan solo debe entregárselos si se los solicita.
7. Recuerde que la Agencia Española de Protección de Datos no almacena la información que usted haya introducido en esta herramienta.

Ha completado con éxito el programa.

A continuación se procederá a la descarga del documento generado con la información que ha incluido en el programa.

Facilita.docx

HERRAMIENTA 2: FACILITA EMPRENDE

A continuación se muestran capturas de pantalla con ejemplos de los diferentes pasos antes mencionados.

Paso 1: Ver si es una empresa tecnológica e identificar tecnologías y datos

SECCIÓN 1 de 3: IDENTIFICACIÓN DE LA ENTIDAD Y ACTIVIDADES DESARROLLADAS

Marque las opciones que caracterizan a su empresa y al modelo de negocio que desarrolla:

De acuerdo con el criterio seguido por el EU Startup Monitor en el estudio de la evolución del ecosistema europeo de emprendimiento, una empresa, para ser considerada startup, debe cumplir los siguientes requisitos:

- Tener un máximo de 10 años de antigüedad
- Mostrar un fuerte carácter innovador en productos y servicios
- Contar con expectativas de crecimiento del número de empleados o de los mercados en los que opera.

¿Considera que su empresa reúne los requisitos enunciados?

- ○ Sí
- ○ No

Marque las tecnologías o desarrollos innovadores que aplican en su modelo de negocio:

- ☐ Plataformas colaborativas
- ☐ Marketplace y/o comercio electrónico
- ☐ Desarrollo de soluciones SaaS (Software as a Service)
- ☐ Desarrollo de aplicaciones web/móviles
- ☐ Juegos
- ☐ Análisis masivo de datos
- ☐ Otras

Nombre o razón social de la empresa

N.I.F.:

Dirección completa de la empresa a efectos legales ***(vía, número, código postal, localidad y provincia)***

Teléfono

Dirección de correo electrónico:

Enlace:
https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQwMjY4MzAxNjUxOTI3NzM2MjM5?updated=true

Andrea Sánchez. Pérez-Llorca.

HERRAMIENTA 2: FACILITA EMPRENDE

A continuación se muestran capturas de pantalla con ejemplos de los diferentes pasos antes mencionados.

Paso 2: Recogida de información sobre los tratamientos llevados a cabo por la empresa tecnológica

SECCIÓN 2 de 3: ANÁLISIS BÁSICO DE LOS TRATAMIENTOS

Aplicando la terminología del Reglamento Europeo de Protección de Datos, usted es **responsable de un tratamiento** cuando es quien decide acerca de la finalidad a la que se destinan los datos o informaciones que pueda recopilar relativas a personas físicas y cuando toma decisiones acerca de los medios o formas en los que dichos datos o informaciones personales van a ser tratados o procesados. En este caso, como responsable de un tratamiento de datos personales, debe de abordar todas las obligaciones señaladas en el RGPD y en la LOPDGDD.

Por el contrario, si en el marco de una relación contractual, usted procesa datos o informaciones personales relativas a personas físicas a requerimiento o solicitud de un tercero que es quién decide sobre la finalidad y los medios o formas en la que los datos van a ser procesados, siguiendo sus instrucciones en todo momento, entonces usted es **encargado de tratamiento**.

Además, en calidad de startup, su empresa podría estar realizando el diseño y desarrollo de productos y servicios adquiridos posteriormente por terceros, ya sean responsables o encargados, actuando como **desarrollador o fabricante** de productos tecnológicos en el contexto de lo que podemos denominar la economía digital. Aunque en ese caso no juegue un papel de responsabilidad desde el punto de vista de las obligaciones del RGPD, pueden resultarle de utilidad las pautas facilitadas en la documentación generada por la herramienta a la hora de incorporar a sus productos aquellas estrategias de diseño y opciones de configuración que ayuden a responsables y encargados a cumplir con sus obligaciones en materia de protección de datos.

En base a lo indicado, seleccione de las siguientes opciones aquellas en las que considera que se desarrollan sus actividades empresariales en las que se tratan o procesan datos y/o informaciones personales:

- ☐ Soy responsable
- ☐ Soy encargado
- ☐ Soy desarrollador

SECCIÓN 2 de 3: ANÁLISIS BÁSICO DE LOS TRATAMIENTOS

¿Su startup trata datos personales de potenciales clientes (personas físicas)?

Se refiere a datos personales de aquellas personas físicas con la que usted todavía no mantiene una relación comercial.

◉ Sí ○ No

A continuación marque qué datos personales trata de sus potenciales clientes

- ☐ Datos de identificación (nombre, apellidos, NIF, dirección postal, teléfono, email)
- ☐ Características personales (estado civil, fecha y lugar de nacimiento, edad, género, nacionalidad)
- ☐ Datos profesionales (cargo, lugar de trabajo, sector de actividad)

Marque de donde obtiene los datos personales de su potenciales clientes

- ☐ Los facilitan ellos
- ☐ Los compro a una tercera empresa

SECCIÓN 2 de 3: ANÁLISIS BÁSICO DE LOS TRATAMIENTOS

¿Su startup trata datos personales de proveedores (personas físicas)?

Se refiere a datos personales de aquellas personas físicas que le proveen de productos o servicios necesarios para su actividad como entidad empresarial (servicios de cloud, alojamiento web, servicios de IA, hardware, software, etc.), proveedor de hardware o cualquier otro producto.

◉ Sí ○ No

A continuación marque qué datos personales trata de sus proveedores

- ☐ Datos de identificación (nombre, apellidos, dirección postal, teléfono, email)
- ☐ Datos bancarios (número de cuenta corriente de abono)

Marque para qué utiliza los datos personales que solicita a sus proveedores

Introduzca otras finalidades:

Finalidad 1

HERRAMIENTA 2: FACILITA EMPRENDE

A continuación se muestran capturas de pantalla con ejemplos de los diferentes pasos antes mencionados.

Paso 3: Análisis de aquellas actividades de tratamiento que se soportan sobre las tecnologías empleadas por la empresa, para caracterizar el nivel de riesgo que representan

SECCIÓN 3 de 3: ANÁLISIS DE TRATAMIENTOS BASADOS EN NUEVOS DESARROLLOS TECNOLÓGICOS Y SOLUCIONES INNOVADORAS

TIPOS DE DATOS

Marque los tipos de datos que trata su empresa en este tratamiento

- ☐ Datos que revelen origen étnico o racial
- ☐ Datos de opiniones políticas o religión
- ☐ Datos de afiliación sindical (excepto cuotas sindicales)
- ☐ Datos genéticos
- ☐ Datos biométricos dirigidos a identificar de manera unívoca a una persona
- ☐ Datos de salud física o mental (excepto grado de discapacidad)
- ☐ Datos relativos a la vida sexual o a la orientación sexual
- ☐ Datos de servicios sociales
- ☐ Datos relativos a condenas penales
- ☐ Datos relativos a la situación financiera o patrimonial
- ☐ Datos sobre preferencias o intereses personales
- ☐ Datos sobre el comportamiento de las personas

SECCIÓN 3 de 3: ANÁLISIS DE TRATAMIENTOS BASADOS EN NUEVOS DESARROLLOS TECNOLÓGICOS Y SOLUCIONES INNOVADORAS

FACTORES DE RIESGO DE LOS TRATAMIENTOS

Marque los factores de riesgo que afectan a este tratamiento

- ☐ ¿Se recaban datos o información de personas en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), relativos a varios aspectos de su personalidad o sus hábitos?
- ☐ Partiendo de la información recopilada ¿se lleva a cabo la toma de decisiones automatizadas o la toma de decisiones que contribuyan en gran medida a la toma de tales decisiones automatizadas, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato?
- ☐ ¿Se lleva a cabo labores de observación, monitorización, supervisión, geolocalización o seguimiento/control de personas de forma directa o indirecta y de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, seguimiento de vehículos, etc.?
- ☐ **¿Realiza alguno de los siguientes tratamientos?**
  - ¿Recopila o procesa información sobre personas relativa a informaciones de tipo étnico o racial, opiniones de índole política, información sobre convicciones religiosas o filosóficas, afiliación sindical, información de tipo genético, información biométrica que permita identificar de manera unívoca a una persona física, datos de salud, información sobre la vida sexual o la orientación sexual?
  - ¿Trata datos relativos a condenas o infracciones penales?
  - ¿Lleva a cabo análisis para determinar la situación financiera o patrimonial de las personas?
  - ¿Lleva a cabo actividades que permitan deducir alguna de las informaciones mencionadas sobre personas físicas?
- ☐ ¿Se realizan actividades en las que se tratan o procesan datos o informaciones biométricas para identificar unívocamente a las personas?
- ☐ ¿Se almacenan o procesan datos genéticos con algún fin?

SECCIÓN 3 de 3: ANÁLISIS DE TRATAMIENTOS BASADOS EN NUEVOS DESARROLLOS TECNOLÓGICOS Y SOLUCIONES INNOVADORAS

FINALIDADES

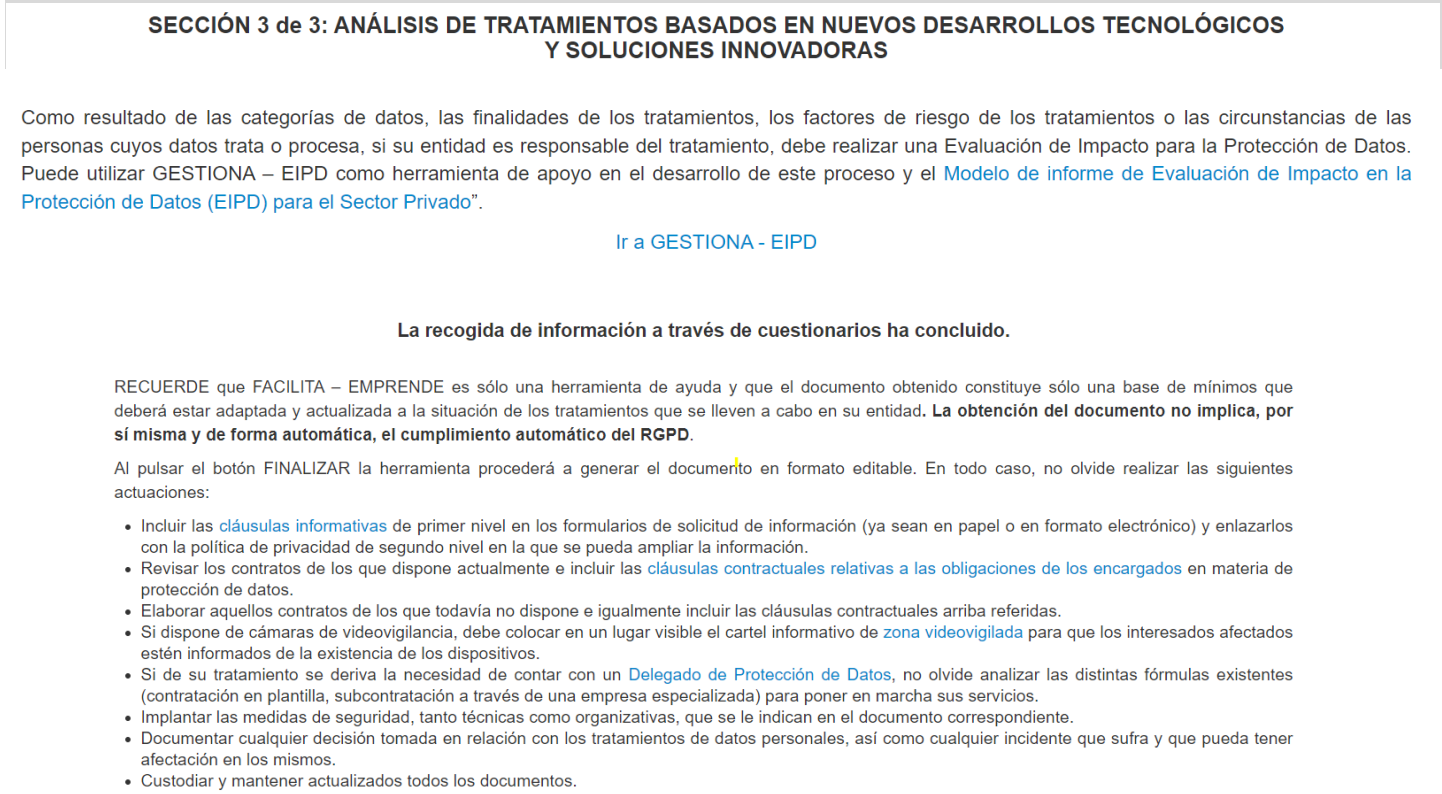
Marque las finalidades que persigue su entidad con este tratamiento

- ☐ Geolocalización
- ☐ Hacer o analizar perfiles
- ☐ Hacer publicidad y prospección comercial masiva a potenciales clientes
- ☐ Gestionar los asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical
- ☐ Gestión, control sanitario o venta de medicamentos
- ☐ Mantenimiento y gestión de historiales clínicos o sanitarios en el marco de investigación sanitaria
- ☑ Mantenimiento de plataformas colaborativas
- ☐ Prestación de servicios a través de un marketplace y/o comercio electrónico
- ☐ Desarrollo de aplicaciones web/móviles/juegos dirigidas a múltiples potenciales usuarios
- ○ Ninguno de los anteriores

RESULTADOS

Como resultado final, la herramienta de FACILITA EMPRENDE te facilita:

- El saber si procede o no realizar una gestión del riesgo y una evaluación de impacto por ser el tratamiento de los datos que lleva a cabo la empresa tecnológica de alto riesgo.
- Documentación para cumplimentar con las obligaciones en materia de protección de datos (cláusulas de firmantes, cartel de video vigilancia, etc.) con los datos cumplimentados. Esta documentación puede ser descargada en formato Word por la empresa (editable).



SECCIÓN 3 de 3: ANÁLISIS DE TRATAMIENTOS BASADOS EN NUEVOS DESARROLLOS TECNOLÓGICOS Y SOLUCIONES INNOVADORAS

Como resultado de las categorías de datos, las finalidades de los tratamientos, los factores de riesgo de los tratamientos o las circunstancias de las personas cuyos datos trata o procesa, si su entidad es responsable del tratamiento, debe realizar una Evaluación de Impacto para la Protección de Datos. Puede utilizar GESTIONA – EIPD como herramienta de apoyo en el desarrollo de este proceso y el Modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) para el Sector Privado".

Ir a GESTIONA - EIPD

La recogida de información a través de cuestionarios ha concluido.

RECUERDE que FACILITA – EMPRENDE es sólo una herramienta de ayuda y que el documento obtenido constituye sólo una base de mínimos que deberá estar adaptada y actualizada a la situación de los tratamientos que se lleven a cabo en su entidad. **La obtención del documento no implica, por sí misma y de forma automática, el cumplimiento automático del RGPD**.

Al pulsar el botón FINALIZAR la herramienta procederá a generar el documento en formato editable. En todo caso, no olvide realizar las siguientes actuaciones:

- Incluir las cláusulas informativas de primer nivel en los formularios de solicitud de información (ya sean en papel o en formato electrónico) y enlazarlos con la política de privacidad de segundo nivel en la que se pueda ampliar la información.
- Revisar los contratos de los que dispone actualmente e incluir las cláusulas contractuales relativas a las obligaciones de los encargados en materia de protección de datos.
- Elaborar aquellos contratos de los que todavía no dispone e igualmente incluir las cláusulas contractuales arriba referidas.
- Si dispone de cámaras de videovigilancia, debe colocar en un lugar visible el cartel informativo de zona videovigilada para que los interesados afectados estén informados de la existencia de los dispositivos.
- Si de su tratamiento se deriva la necesidad de contar con un Delegado de Protección de Datos, no olvide analizar las distintas fórmulas existentes (contratación en plantilla, subcontratación a través de una empresa especializada) para poner en marcha sus servicios.
- Implantar las medidas de seguridad, tanto técnicas como organizativas, que se le indican en el documento correspondiente.
- Documentar cualquier decisión tomada en relación con los tratamientos de datos personales, así como cualquier incidente que sufra y que pueda tener afectación en los mismos.
- Custodiar y mantener actualizados todos los documentos.

HERRAMIENTA 3: GESTIONA EIPD

A continuación se muestran capturas de pantalla del proceso de EIPD. En este caso sólo se muestran capturas de la fase de las 8 preguntas para determinar el riesgo que entraña el tratamiento de los datos y si se precisa hacer una evaluación de impacto; pues como ya comentamos la parte de preguntas sobre la identificación de los riesgos y cómo se manejan son idénticas a las que se hacen en el proceso gestión de los riesgos que contaremos a continuación.

A continuación se muestran capturas de pantalla ejemplificativas de los pasos antes mencionados:

// DIPLOMA

Unai Sánchez Martínez, como Presidente de la **Coordinadora de ONG para el Desarrollo de la Región de Murcia (CONGDRM)**, con CIF G-304 82 640, registrada con el número 3797 en el Registro de Asociaciones de la Región de Murcia, y Leire Larracoechea San Sebastián, como Directora Ejecutiva de la **Fundación Pro Bono España (FPBE)**, con CIF G-88151964, registrada con el número 2150 en el Registro de Fundaciones Estatal,

Otorgan el presente Diploma a

Haga clic o pulse aquí para escribir texto., en representación de Haga clic o pulse aquí para escribir texto., por su **PARTICIPACIÓN** online en los talleres formativos del programa gratuito **"Modo dataprotectiON"** para entidades sin ánimo de lucro del Tercer Sector, celebrados del 20 de enero al 23 de junio de 2022.

Y firman a los efectos oportunos, a 12 de julio de 2022:

Unai Sánchez Martínez
Presidente de la CONGDRM

Leire Larracoechea San Sebastián
Directora Ejecutiva de la FPBE

Coordinadora ONGD Región de Murcia · Región de Murcia · AGENDA 2030 POR UN DESARROLLO HUMANO SOSTENIBLE · Fundación Pro Bono España //

ABOGADOS Y ABOGADAS RESPONSABLES DEL PROGRAMA FORMATIVO "MODO DATA PROTECTION"

María Luisa González Tapia es asociada del Departamento de IT/IP de Ramón y Cajal Abogados. Se incorporó a dicha firma en 2014, tras una trayectoria de más de 10 años en distintas consultoras y despachos. Está especializada en protección de datos, propiedad intelectual relacionada con las nuevas tecnologías, comercio electrónico, contratación a distancia, contratación informática, y asesoramiento a desarrolladores de redes sociales y "apps". Se licenció en Derecho en la Universidad San Pablo-CEU de Madrid, completando su formación con un Master en Derecho de las Tecnologías de la Información y Comunicaciones en ICADE. Es abogada en ejercicio del Ilustre Colegio de Abogados de Madrid desde el año 2000. María Luisa ha participado en proyectos de larga duración de privacidad, compliance y seguridad de la información en diversas multinacionales y Administraciones Públicas. Asimismo, dispone de una amplia experiencia realizando auditorías de protección de datos y medidas de seguridad a organizaciones de sectores como el de la energía, el sanitario, el tecnológico o el del transporte. Es CIPP/US, CIPP/E, Lead Auditor 27001 y Lead Auditor BS 25999. Ha sido reconocida por Chambers Europe, Legal500 y Best Lawyers.

Antonio Borjas es abogado del Departamento de IT/IP de Ramón y Cajal Abogados. Está especializado en protección de datos, seguridad de la información y comercio electrónico, contando con la certificación de Delegado de Protección de Datos conforme al esquema AEPD – DPD y con la certificación de Compliance CESCOM. Se graduó en Derecho en la Universidad Carlos III de Madrid, completando su formación con un Master en Ejercicio de la Abogacía impartido por la Universidad Carlos III de Madrid y el ISDE, así como con diferentes cursos en materia de protección de datos y compliance. Es abogado en ejercicio del Ilustre Colegio de Abogados de Madrid y asociado de la APEP. Antonio asesora en proyectos de implementación de la normativa de protección de datos en diferentes compañías, elaborando los correspondientes registros de actividades de tratamiento y redactando diferentes políticas y cláusulas de privacidad. Asimismo, participa en auditorias de protección de datos y asesora en la realización de evaluaciones de impacto y análisis de riesgos. Gestiona diferentes buzones de ejercicios de derechos ARCO-PLUS e imparte cursos de formación en materia de privacidad.

Pablo Tena se formó como abogado en la Universidad de Zaragoza y en la Universidad de Navarra. Es abogado especializado en privacidad desde hace seis años, y ha asesorado a empresas nacionales e internacionales en todo tipo de consultas y proyectos relacionados con esta materia. La mayor parte de su carrera profesional ha estado vinculada al Despacho Ramón y Cajal y, actualmente, se encuentra en Cuatrecasas.

Lidia Vidal es Asociada Senior del departamento de TMT en Pinsent Masons Madrid. Está especializada en Derecho de propiedad industrial e intelectual y Derecho de las tecnologías de la información, contando con una amplia experiencia en marcas, Derecho de la publicidad, protección de datos y comercio electrónico en diversos sectores. Lidia asesora habitualmente a clientes nacionales y multinacionales en sectores como retail, salud, servicios financieros y tecnología. Presta asesoramiento jurídico en asuntos no contenciosos, incluyendo la negociación de contratos comerciales con un elemento de IP o IT, la adaptación de plataformas tecnológicas a la normativa de protección de datos y comercio electrónico, así como en asuntos relacionados con derechos de imagen, consumidores y usuarios, publicidad digital o ciberseguridad. Asimismo, su experiencia incluye el asesoramiento y defensa ante los juzgados y tribunales. En particular, ha participado en complejos procedimientos relacionados con la infracción, nulidad y caducidad de marcas y diseños industriales.

María Gutiérrez-Bolívar es abogada del departamento de TMT en Pinsent Masons Madrid. Está especializada en las áreas de Propiedad Intelectual, Telecomunicaciones y Tecnologías de la Información. María ha asesorado a empresas líderes, tanto a nivel local como internacional, centradas en los sectores de Energía, Telecomunicaciones, Data Centers, Transporte y Financiero. Concretamente, ha asesorado en cuestiones relacionadas con el cumplimiento de la normativa europea y local en materia de protección de datos sobre: transferencias internacionales, el diseño de páginas web, la monetización de los datos, contratos tecnológicos y de privacidad y las brechas de seguridad. También asesora en materia de contratación electrónica relacionada con los servicios financieros. Y ofrece asesoramiento jurídico en relación la preparación de ofertas públicas y las autoridades reguladoras. María también ha participado en el desarrollo de nuevos productos jurídicos innovadores como la plataforma global de gestión de brechas de la firma.

Andrea Sánchez trabaja en el departamento de Propiedad Intelectual, Industrial y Tecnología del despacho Pérez-Llorca. Sus áreas de práctica comprenden el asesoramiento relacionado con propiedad industrial e intelectual, protección de datos y comercio electrónico. Concretamente, ha asesorado a empresas de diversos sectores en proyectos internacionales y multidisciplinares en relación con la adecuación al Reglamento Europeo de Protección de Datos, así como en todas aquellas actividades que tienen como activo los datos personales. Por otro lado, asesora en la redacción, revisión y negociación de contratos de software, elaboración de contratos de licencia, mantenimiento y soporte de software, acuerdos ANS y en la elaboración y negociación de contratos de publicidad o patrocinio. Andrea también ha prestado asesoramiento a clientes nacionales en diferentes cuestiones, incluyendo litigios en materia de Competencia Desleal.

Como abogado de Pérez-Llorca experto en tecnología e intangibles, **Andy Ramos** presta asesoramiento en la identificación, protección, transmisión y adquisición de activos intangibles, incluyendo obras y prestaciones creativas, marcas, patentes, datos o secretos empresariales. Asimismo, Andy es cofundador y responsable institucional de la Asociación Española de Derecho del Entretenimiento (DENAE).

Manel Santilari se incorpora en 2012 al departamento de Litigación y Propiedad Intelectual e Industrial de Clifford Chance, donde se ha especializado en protección de datos personales, derecho de los consumidores, así como en asesoramiento en litigios multi jurisdiccionales de patentes, litigación comercial y competencia desleal. En relación con la protección de datos, asesora diariamente a multinacionales en aspectos clave de sus negocios relacionados con los datos personales (análisis y revisión de bases jurídicas legitimadoras, cláusulas informativas, comunicaciones comerciales, cesiones de datos personales, transferencias internacionales, entre otros), en requerimientos de información y procedimientos sancionadores frente a la AEPD, así como en transacciones societarias de todo tipo. También asesora de forma habitual y con carácter pro bono a diferentes asociaciones y fundaciones sin ánimo de lucro en cuestiones relacionadas con la protección de datos personales.

Desde que se incorporó a Clifford Chance (2005), **Sònia Sebé** ha asesorado a empresas nacionales e internacionales en materia de derechos de Propiedad Intelectual e Industrial, Protección de Datos, Publicidad y Compliance. Colabora regularmente en sesiones informativas y cursos sobre Propiedad Industrial y Protección de Datos en instituciones como la Universitat Pompeu Fabra o el Instituto Superior de Derecho y Economía (ISDE). En lo que se refiere a protección de datos, presta asesoramiento de forma regular a empresas nacionales e internacionales, incluyendo la redacción y revisión de contratos y cláusulas informativas, la redacción de escritos para su presentación ante la Agencia Española de Protección de Datos (AEPD), el asesoramiento en materia de brechas de seguridad, asesoramiento en procedimientos sancionadores ante la AEPD y en procedimientos de "due diligence".

OPINIONES DE LOS PARTICIPANTES

"*Las entidades del tercer sestor han podido resolver, con este curso, parte de sus dudas y han obtenido modelos prácticos que les ayudarán en la gestión del día a día de sus organizaciones. Lo mejor de todo es que la Fundación Pro-Bono España continuará dando soporte a las mismas personas que hemos formado. Este será el principio de una red de soporte continuado y específico en materia de protección de datos para el tercer sector.*" Maria Luisa González (abogada en Ramón y Cajal Abogados)

"La colaboración en el programa Data ProtectiON ha sido enriquecedora al poder conocer de primera mano las necesidades específicas de las entidades del tercer sector Además, ha sido gratificante poder proponer un programa para que, con los recursos materiales y humanos con los que cuentan las entidades sociales, puedan cumplir con los principios y obligaciones básicos de privacidad y, con ello, facilitar su labor fundamental que desempeñan en nuestra sociedad." Antonio Borjas (abogado en Ramón y Cajal Abogados)

"Uno de los aspectos clave del programa es que está orientado a acercar de forma práctica y efectiva la protección de datos, un área de Derecho que suele generar dudas por su carácter técnico y novedoso, a las entidades no lucrativas. Las sesiones del programa van más allá del plano teórico y ofrecen una serie de sesiones prácticas que implican un acompañamiento completamente personalizado, facilitando la participación de las entidades para plantear a los abogados las cuestiones que afectan a su día a día." Lidia Vidal (abogada en Pinsent Masons)

"El programa Modo dataprotectiON ha ayudado a solventar cuestiones relevantes en materia de protección de datos para este tipo de organizaciones que, por desgracia, suelen tener menos recursos para cuestiones técnicas. El programa nos ha facilitado, por un lado, resolver dudas de cada organización y, por otro lado, formar a los profesionales que las integran para que apliquen los conceptos básicos de protección de datos en el futuro." Pablo Tena (abogado en Ramón y Cajal durante el desarrollo del programa)

"Lo que más destacaría del programa es su metodología. Los talleres no solo han servido a los participantes, sino que los que los hemos preparado también hemos podido aprender cuáles son las principales dificultades de las entidades sin ánimo de lucro a la hora de adaptarse a la normativa aplicable en materia de protección de datos, para, así mejorar nuestro asesoramiento de cara a futuras consultas." María Gutiérrez-Bolívar (abogada en Pinsent Masons)

"*El programa Modo dataprotectiON dio lucidez sobre una materia que afecta a una infinidad de agentes y que, por su repercusión en los derechos y libertades de las personas, exige un cumplimiento estricto de la normativa. Es importante saber qué recursos hay disponibles para facilitar su cumplimiento, pues no deja de ser una materia compleja y difícil de afrontar por gran parte del sector, siendo este tipo de sesiones un canal para fomentar un mayor cumplimiento de la ley*." Andrea Sánchez (abogada en Pérez-Llorca)

"El reto de transmitir en pocas sesiones conocimientos sobre una materia en constante evolución como la protección de datos se ha visto de sobra recompensado por el entusiasmo, interés y ganas de aprender de todos los participantes. Agradecemos a la Fundación Pro Bono España que nos haya brindado esta oportunidad." Manel Santilari (abogado en Clifford Chance)

ENTIDADES SOCIALES BENEFICIARIAS

¿Qué puntuación global otorgarías al curso? (siendo 1 "muy mal" y 10, "perfecto")

9,2/10 ★★★★★

¿Cómo crees que ha sido la organización de la formación? (siendo 1 "muy mal" y 10, "perfecto")

9,2/10 ★★★★★