datalawyers

DE LA LOPD AL RGPD

APLICACIÓN EN DESPACHOS DE ABOGADOS

Normativa

- 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, está en vigor desde el 25 de mayo de 2016 (deroga la Directiva 95/46/CE) y **será de aplicación obligatoria en todos los Estados de la UE a partir del 25 de mayo de 2018 (RGPD)**
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. **(LOPD)**
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD **(RLOPD)**
- Anteproyecto de Ley Orgánica de protección de datos

Conceptos

Conceptos (I)

- **Tratamiento**: "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
- **Fichero:** conjunto estructurado de datos personales susceptibles de tratamiento para un fin determinado.
  - LOPD.- Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso

Conceptos (II)

- **Datos de carácter personal:** "toda información sobre una persona física identificada o identificable", por la cual pueda determinarse, directa o indirectamente su identidad
  - Ejemplo de datos:

    nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona, una fotografía, el sonido de una grabación, la imagen de un vídeo, datos biométricos, imágenes faciales o datos dactiloscópicos
- **Interesado:** "persona física identificada o identificable"

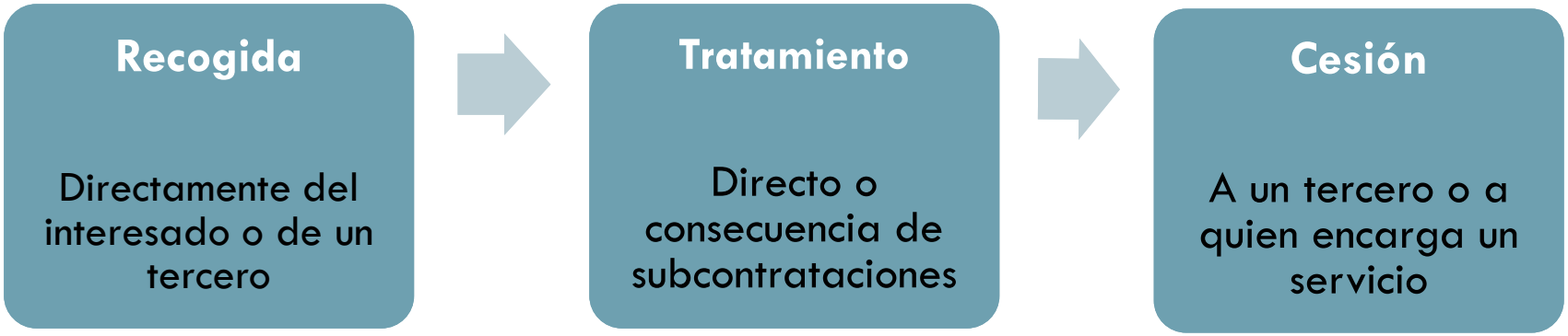
Conceptos (III)

- **Responsable de tratamiento (RT)**: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento
- **Encargado de Tratamiento (ET)**: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento
- **Corresponsable del tratamiento:** cuando varios RT determinen los fines y los medios del tratamiento.
- **Destinatario de datos:** la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

Conceptos (IV)

- **Seudonimización:** el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, debe
  - figurar por separado y
  - sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable
- **Delegado de protección de datos (DPO):**Persona encargada de informar y asesorar al RT, ET y al Personal autorizado de las obligaciones relativas a la protección de datos personales
- **Autoridad de control (AC):** la autoridad pública independiente establecida por un Estado miembro (Agencia Española de Protección de Datos)

Tratamiento de datos



Principios que rigen el tratamiento de datos: información, licitud, lealtad y transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad, responsabilidad proactiva

Tratamiento de datos

Principios

Tratamiento de datos_ Principios (I)

- **Licitud, lealtad y transparencia,** para fines específicos o sean recogidos con **fines determinados, explícitos y legítimos** y no tratados posteriormente de manera incompatible con dichos fines.
- La **minimización de datos,** siendo adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados
- La **exactitud, confidencialidad, integridad, seguridad física** y supresión de los datos.
- La protección de los **derechos del interesado.**
- Que los datos no sean accesibles, sin la intervención humana, a un número indeterminado de personas.

Tratamiento de datos_ Principios (II)

Consentimiento del interesado: "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o clara acción afirmativa, el tratamiento de datos personales que le conciernen"

- El tratamiento de datos personales debe basarse, de forma general, en el consentimiento libre, informado, específico e inequívoco del interesado
  - LOPD consentimiento "tácito", "expreso" y "expreso y por escrito" verificable
- Requisitos: información específica, antes de iniciarse el tratamiento, inequívoco, libremente otorgado
- Condiciones: el RT asume la prueba, verificable, debe de ser fácil de retirar

Tratamiento de datos_ Principios (III)

Tratamiento de categorías especiales de datos personales

"Quedan prohibidos los tratamientos de 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"

Tratamiento de datos_ Principios (IV)

Excepciones:

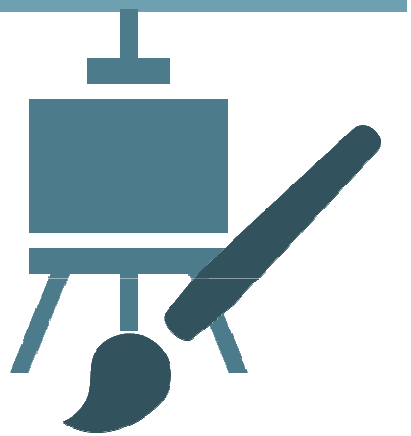
- el interesado dio su consentimiento explícito,
- es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del RT o del interesado en el ámbito del Derecho laboral y de la SS
- para proteger intereses vitales del interesado o de otra persona
- para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función
- por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros y por razones de interés público en el ámbito de la salud pública
- para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social

Tratamiento de datos_ Principios (V)

- **Protección de datos desde el diseño y por defecto**

  El Responsable del tratamiento deberá garantizar:

  - desde el diseño y por defecto,
  - antes y durante el tratamiento
  - la aplicación efectiva de los principios de protección de datos
    - a todos datos personales tratados, así como
    - al plazo de conservación y
    - a su accesibilidad



- Sometido al **principio de responsabilidad proactiva**: siendo responsable y capaz de demostrar el cumplimiento de todos los principios del tratamiento

Tratamiento de datos_ Principios (VI)

Información al interesado (claramente informado del tratamiento)

- De forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo
- En el momento de la obtención de los datos
- Si está previsto comunicarlos a un destinatario, la información se deberá facilitar al interesado, como máximo, en el momento en que los datos los comuniquemos por primera vez al destinatario
- No es necesario comunicar la información al interesado:
  - cuando el interesado ya disponga de la información
  - cuando la comunicación sea imposible o suponga un esfuerzo desproporcionado

El RT deberá diseñar políticas concisas, transparentes, sencillas y accesibles para comunicar al interesado los detalles del tratamiento y el ejercicio de los derechos sobre sus datos

Tratamiento de datos_ Recogida de datos

Le informamos que los datos personales recogidos en el momento de la ***contratación*** *(base jurídica del tratamiento), los comunicados a lo largo de la duración del contrato y aquellos que comunique en el futuro para el cumplimiento de sus obligaciones legales, serán tratados bajo la* ***responsabilidad de ..... (identidad y datos de contacto del RT y/o DPO)*** *con el* ***fin*** *(finalidades del tratamiento) de gestionar la relación laboral que los une. (plazo del conservación o criterios que lo determinen)*

Le informamos que los datos ***no serán comunicados*** *(destinatarios) a terceros, salvo obligación legal y que podrá ejercer los* ***derechos*** *(derechos de los interesados) de acceso, rectificación, portabilidad y supresión de sus datos y los de limitación y oposición a su tratamiento dirigiéndose a..... o enviando un mensaje al correo electrónico a .....Si considera que el tratamiento no se ajusta a la normativa vigente, podrá presentar una reclamación ante la autoridad de control en agpd.es.*

(Si los datos no son obtenidos del interesado, también se informará sobre la fuente de procedencia de los datos y las categorías de datos tratados)

Prestaciones de servicios_ Cesión

- El ET o cualquier persona que actúe bajo la autoridad del RT o del ET y tenga acceso a los datos solo podrá tratar dichos datos siguiendo las instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la UE o EM
- La relación con el RT se rige por un **contrato u otro acto jurídico**

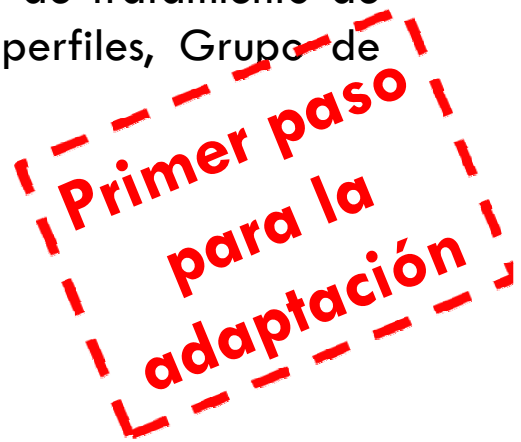
Prestaciones de servicios_ Acuerdo

Contenido mínimo del **acuerdo:**

- Objeto
- Duración
- Naturaleza
- Finalidad del tratamiento
- Tipo de datos personales
- Categoría de interesados
- **Obligaciones y derechos del responsable y del encargado de tratamiento**
- En particular: identificación de los tratamientos, deber de confidencialidad, medidas de seguridad a aplicar, régimen de subcontratación, derechos de los interesados, colaboración de cumplimiento, destino de los datos al finalizar la prestación y colaboración para demostrar el cumplimiento

Tratamiento de datos en el despacho (I)

- Identificar los datos personales
- Estructurarlos en según su finalidad.
- Asignar a cada fichero/tratamiento una categoría de datos
- Asignar a cada fichero la responsabilidad del tratamiento RT/ET
- Analizar si a algún fichero le corresponde alguna categoría de tratamiento de Alto riesgo, Transferencias internacionales, Elaboración de perfiles, Grupo de empresas y Titularidad o interés público.
- Comprobar el cumplimiento de los principios del tratamiento.



Tratamiento de datos en el despacho (II)

Es necesaria la llevanza del **Registro de actividades** cuando se dé alguna de las siguientes circunstancias:

- Empleen a un mínimo de 250 personas.
- Realicen habitualmente tratamientos que puedan suponer un riesgo para los interesados.
- Traten categorías especiales de datos.
- Traten datos relativos a condenas y delitos penales

Atención de los derechos de las personas
Notificación de quiebras de seguridad

Tratamiento de datos_ Registro de Actividades

A **disposición de la Autoridad de control**
Formato: papel o electrónico
Contenido:

- ✓ Identificación de: ET, RT, CT, y si es el caso, Coencargados, Destinatarios, Representantes y DPO
- ✓ Identificación de los tratamientos efectuados y categorías de datos (descripción y plazos previstos)
- ✓ Categorías de destinatarios, incluyendo organizaciones internacionales y terceros países
- ✓ Descripción general de medidas técnicas y organizativas, si es posible

Tratamiento de datos _medidas de seguridad

Responsabilidad proactiva: El RT, **antes y durante el tratamiento,** deberá aplicar **medidas de protección de datos proporcionadas** en relación con las actividades del tratamiento e implementar medidas técnicas y organizativas apropiadas para **garantizar y demostrar el cumplimiento del RGPD,** teniendo en cuenta:

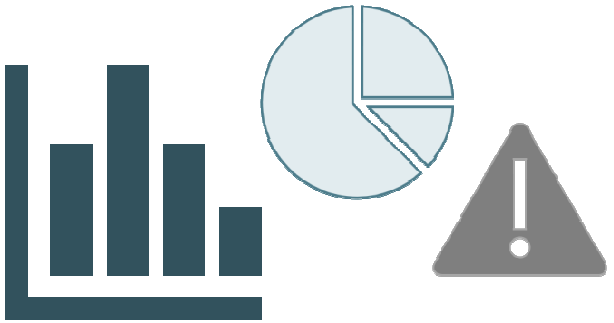
- La naturaleza, ámbito, contexto, y fines del tratamiento.
- Los riesgos para los derechos y libertades de los interesados.
- El tipo de organización

Revisión y actualización

Tratamiento de datos_ Análisis de riesgos

Para **evaluar el nivel de seguridad a implantar** en la organización se analizarán los riesgos que entrañe el tratamiento como consecuencia de:

- La destrucción accidental o ilícita de datos.
- La pérdida, alteración o comunicación no autorizada.
- El acceso a los datos cuando sean transmitidos, conservados u objeto de algún otro tipo de tratamiento.



Tratamiento de datos_ Análisis de riesgos

Medidas de protección de datos

- Seudonimización o cifrado de datos personales
- Confidencialidad, integridad, disponibilidad y resistencia de los sistemas de tratamiento.
- Acuerdos de confidencialidad con el personal autorizado para el tratamiento de datos.
- Restauración de datos mediante copias de respaldo.
- Auditoría de las medidas de seguridad adoptadas

Alto riesgo

- Evaluación de impacto
  - Informe: descripción sistemática de las operaciones de tratamiento previstas/evaluación de la necesidad y proporcionalidad el tratamiento, evaluación de riesgos, garantías de protección para los derechos de los interesados, medidas de seguridad prevista para afrontar los riesgos y revisión

Tratamiento de datos_ Análisis de riesgos

Extracto del informe "ANÁLISIS DE LOS RIESGOS DEL TRATAMIENTO"

De conformidad con el artículo 32 del Reglamento (UE) 2016/679 de 27 de abril de 2016 (GDPR), se ha analizado el nivel de seguridad a implantar en la Organización para garantizar la protección de datos, teniendo en cuenta los altos riesgos que pueda tener el tratamiento para los derechos y libertades de los interesados, como consecuencia de:

- *La destrucción accidental o ilícita de datos.*
- *La pérdida, alteración o comunicación no autorizada.*
- *El acceso a los datos cuando sean transmitidos, conservados u objeto de algún otro tipo de tratamiento.*

Para ello, se ha analizado la probabilidad de riesgos que conlleva el tratamiento en tres apartados:

- *Estructura de los datos.*
- *Cumplimiento del Reglamento.*
- *Seguridad del tratamiento*

La probabilidad de riesgos se ha clasificado de la siguiente forma:

- *Muy bajo (tratamiento sin riesgos) - **1***
- *Bajo (tratamiento con pocos riesgos y asumible si se cumple la normativa de protección de datos) - **2.***
- *Medio (tratamiento susceptible de algún riesgo, que precisa de procesos de verificación de las medidas adoptadas) -**3***
- *Alto (tratamiento susceptible de un alto riesgo, que precisa valorar la necesidad de realizar una evaluación de impacto) **-4***
- *Muy Alto (tratamiento con un alto riesgo, que precisa realizar una evaluación de impacto)- **5.***

Ejemplo

Tratamiento de datos_ quiebras de seguridad

- El RT deberá **documentar cualquier violación de la seguridad** de los datos personales producida bajo su responsabilidad **y notificarla a la AC,** sin dilación indebida, a ser posible en un **máximo de 72 horas** desde que se haya tenido constancia de ella, salvo una justificación motivada que acompaña a la notificación.
- Cuando la violación se haya producido bajo la responsabilidad del ET, éste lo notificará al RT sin dilación indebida
- **No será necesario notificar** una violación de datos a la Autoridad de control **cuando sea improbable que la vulneración de los datos personales constituya un riesgo para los derechos y las libertades de los interesados**

Tratamiento de datos_ quiebras de seguridad

Registro de quiebras de seguridad:

- La naturaleza y contexto de la violación.
- Los posibles efectos y consecuencias de la violación.
- Las medidas correctivas
- Cuando sea posible las categorías y número de interesados y registros afectados.
- Si es el caso, la identidad y los datos de contacto del DPO u otros contactos para obtener más información.
- Si no es posible facilitar toda la información en una comunicación, se notificará por etapas sin dilación indebida

Tratamiento de datos_ quiebras de seguridad

El RT comunicará una violación de datos al interesado, sin dilación indebida, cuando :

- Sea probable que presente un alto riesgo
- Le sea exigido por la Autoridad de control

Excepción, cuando pueda demostrar:

- Que se han adoptado y aplicado medidas apropiadas de protección para hacer ininteligibles los datos a personas no autorizadas
- Que se garantiza que no es probable un alto riesgo
- Que supone un esfuerzo desproporcionado. Se podrá optar por una comunicación pública que sea igualmente efectiva para informar al interesado

Tratamiento de datos_ quiebras de seguridad

Una descripción de la naturaleza de la violación		
Las posibles consecuencias de la violación		
Medidas correctivas adoptadas o propuestas por el RT para remediar y mitigar los efectos ocasionados.		
Identidad y los datos de contacto del DPO u otros contactos para obtener más información	Nombre y apellidos	
	Dirección de contacto	
	Email	

Ejemplo

Tratamiento de datos_ quiebras de seguridad

Ejemplos de quiebras de seguridad

- Acceso no autorizado a los sistemas informáticos
- Transmisión ilícita de datos a un Destinatario
- Vulneración del secreto profesional
- Envío de correos electrónicos masivos sin ocultar los destinatarios
- Robo o sustracción de información
- Incendio, inundación u otras causas ajenas a la empresa
- Falsificación de datos

Tratamiento de datos_ DPO

Perfil: conocimientos especializados en derecho y práctica en PD, en plantilla o contratado, sus datos se comunicarán a las autoridades de control

Notificación a la AC (ya disponible online)

Funciones:

- Comunicarse con las autoridades de control
- Establecer mecanismos para que los ciudadanos puedan contactarle
- Asesoramiento en las evaluación de impacto, informar y asesorar al Responsable/ encargado, supervisar cumplimiento normativo

Tratamiento de datos_ DPO

Cuando las actividades principales consistan en operaciones de tratamiento que requieran el seguimiento:

- regular: continuado, recurrente o repetido, en momento prefijado y que se produce de forma constante o periódica
- Y sistemático: sistema preestablecido, organizado o metódico, que tiene lugar como parte de un plan general y llevado a cabo como parte de una estrategia

Cuando las actividades principales consistan en tratamiento a gran escala de datos de categorías especiales

- origen racial o étnico,
- las opiniones políticas,
- las creencias religiosas o filosóficas o
- la pertenencia a sindicatos,
- datos genéticos,
- biométricos para la identificación exclusiva de personas físicas,
- datos relativos a la salud,
- datos referentes a la vida sexual o la orientación sexual de las personas
- Datos personales relacionados con condenas y delitos penales

Derechos de los interesados

Derechos de los interesados

Cualquier tratamiento	Tratamiento automatizado	Otros derechos
• Acceso • Rectificación • Supresión • Limitación • oposición	• Portabilidad • Oponerse a la elaboración de perfiles	• Revocación del consentimiento • Reclamación a la autoridad de control

Derechos de los interesados _ procedimiento

El Responsable del tratamiento deberá crear un **procedimiento para dar curso a los derechos de los interesados** de manera que pueda responder las solicitudes sin demora y garantizar que se ejecutan los derechos conforme el Reglamento:

- Registro de peticiones
- Confirmar la identidad del interesado
- Dar curso a la petición, contestar sin demora
- Resolución, dando la información estructurada

Sanción por incumplimiento: multa administrativa con un máximo del importe más elevado entre 20.000.000 € y el 2% del volumen de negocio total anual global del ejercicio financiero anterior

Derechos de los interesados _ procedimiento

El Responsable del tratamiento deberá crear un **procedimiento para dar curso a los derechos de los interesados** de manera que pueda responder las solicitudes sin demora y garantizar que se ejecutan los derechos conforme el Reglamento:

- Registro de peticiones
- Confirmar la identidad del interesado
- Dar curso a la petición, contestar sin demora
- Resolución, dando la información estructurada

Sanción por incumplimiento: multa administrativa con un máximo del importe más elevado entre 20.000.000 € y el 2% del volumen de negocio total anual global del ejercicio financiero anterior

Autoridad de control (I)

Son las Autoridades públicas dispuestas por un

Estado de la UE destinadas a supervisar la aplicación del RGPD

- con el fin de proteger los derechos y las libertades fundamentales de los interesados:
- en lo que respecta al tratamiento de sus datos personales y
- a facilitar la libre circulación de datos personales en la UE

Autoridad de control (II)

Todo interesado podrá reclamar ante la AC de cualquier Estado de la UE, si considera que el tratamiento de sus datos personales no se ajusta a lo dispuesto en el RGPD

- **Derecho a un recurso judicial contra una AC**
  - Los RT o ET tendrán derecho a un recurso judicial efectivo contra una decisión jurídicamente vinculante de la AC que les afecte.
  - El interesado tendrá derecho a un recurso judicial efectivo en contra de la AC cuando ésta no de curso a una reclamación o no le haya informado en 3 meses.
- **Derecho a un recurso judicial contra un RT o ET**
  - El interesado tendrá derecho a un recurso judicial efectivo contra un RT o ET cuando considere que el tratamiento de sus datos personales no se ajusta a lo dispuesto en el RGPD
  - Las acciones contra el RT y ET podrán ejercitarse ante los órganos jurídicos del Estado de la UE donde:

    Esté establecido el RT o ET

    Resida el interesado siempre y cuando el RT o ET no sea una Autoridad pública que actúe en ejercicio de su poder público.

Plan

Verificación del cumplimiento de los principios del tratamiento

RESPONSABILIDAD PROACTIVA

Recogida, tratamiento y cesión

Licitud, lealtad y transparencia/ limitación de la finalidad/ minimización del dato/exactitud/limitación en el plazo de conservación/ integridad y confidencialidad

Responsabilidad del tratamiento

- Registro de las actividades
- Análisis de riesgos
- Registro de quiebras de seguridad
- Evaluación de impacto
- Aplicación de medidas de protección de datos

En relación a los interesados

- Política de información (clausulas y advertencias legales en hojas de encargo, contratos, etc.)
- Obtención del consentimiento
- (acción positiva)
- Procedimientos de actuación ante el ejercicio de derechos y reclamaciones ante la Autoridad de Control.

Ejemplos prácticos (contenido informe evaluación impacto)

Ejemplo

1. IDENTIFICACIÓN DEL PROYECTO
   - 1.1 Datos identificativos
   - 1.2. Promotor del proyecto
   - 1.3. Generalidades del tratamiento
   - 1.4. Alcance de la evaluación de impacto
   - 1.5. Sistemas de información y tecnologías
   - 1.6. Otras informaciones

2. RESUMEN EJECUTIVO
   - 2.1 Descripción ejecutiva del proyecto
     - 2.1.1 Equipo
     - 2.1.2 Obligación de realizar una DPIA
   - 2.2 Método de evaluación
   - 2.3 Tratamientos con probabilidad de riesgos
   - 2.4. Estructura técnica y organizativa
   - 2.5 Responsabilidades del tratamiento

3. OBJETIVOS Y FINALIDADES DEL TRATAMIENTO
   - 3.1 Base de legitimación del tratamiento
   - 3.2 Fines del tratamiento
   - 3.3 Necesidad y proporcionalidad del tratamiento

4. PROCESO DE CONSULTAS
   - 4.1 Resultado del proceso de consultas
   - 4.2 Identificación de las partes interesadas (internas y externas)
   - 4.3 Mecanismo de consulta y contribución de las partes
   - 4.4 Resumen de los aspectos más relevantes derivados de la consulta

5. DESCRIPCIÓN DETALLADA DEL PROYECTO
   - 5.1 Descripción general del tratamiento
   - 5.2 Descripción detallada del tratamiento
   - 5.3 Principales riesgos detectados
   - 5.4. Medidas propuestas para mitigar los riesgos
   - 5.5 Necesidad de realizar una consulta previa

6. IDENTIFICACIÓN Y GESTIÓN DE RIESGOS
   - 6.1 Identificación detallada de riesgos
   - 6.2 Impacto y probabilidad de riesgos
   - 6.3 Mapa de riesgos
   - 6.4 Análisis de cumplimiento normativo

7. CONCLUSIONES
   - 7.1 Análisis final
   - 7.2 Recomendaciones
   - 7.3 Resumen de medidas a implantar

8. ANEXOS
   - 8.1 Proceso de implantación de las medidas propuestas
   - 8.2 Revisión de la evaluación de impacto
   - 8.3 Conceptos y definiciones

Ejemplos prácticos (aplicación de medidas de protección de datos- delitos y condenas penales)

El tratamiento de datos penales comporta el cumplimiento de todas las disposiciones del GDPR relativas a la categoría de datos tratados básicos, teniendo en cuenta las siguientes particularidades:

Legitimación del tratamiento

- Tratamiento fundamentado en la legislación vigente:
  - Con garantías apropiadas para los derechos y libertades de los interesados
  - Bajo la supervisión de poderes públicos.

Protección de datos desde el diseño y por defecto

- Adoptar medidas adicionales de seguridad:
  - Mecanismos de identificación y autenticación adicionales para limitar el acceso al mobiliario o departamentos.
  - Mecanismos de identificación y autenticación adicionales para acceder a ficheros o aplicaciones informáticas.
  - Mecanismos efectivos que impidan el acceso a información contenida en soportes móviles y trasladables fuera de la empresa.
  - Contraseñas cifradas y seguras (mínimo 12 caracteres, mayúsculas, minúsculas, dígitos, símbolos).
  - Impedir intentos reiterados de acceso no autorizados.
  - Implementar procesos de verificación, evaluación y valoración de las medidas de seguridad adoptadas.

Análisis de riesgos

- Analizar si la actividad principal del RT o ET contempla un tratamiento a gran escala basado en datos relativos a condenas e infracciones penales o medidas de seguridad conexas.
- En el caso de existir un tratamiento a gran escala, se aplicará el protocolo para tratamientos con alto riesgo:
  - Llevar a cabo una evaluación de impacto relativa a la protección de datos.
  - Designar un Delegado de Protección de Datos (DPO).

Registro de las actividades del tratamiento

- Es obligatorio para cualquier RT o ET que realice tratamientos de datos penales

Ejemplo

Ejemplos prácticos (informe responsabilidad proactiva)

Contenido de un informe de responsabilidad proactiva

1. Identificación de la organización Responsable del tratamiento

De conformidad con lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril de 2016 (GDPR) la organización Responsable del tratamiento es quién determina los fines y los medios del tratamiento de datos personales

(…)

2. Identificación de los Fichero/ tratamientos de datos personales

Un fichero es un conjunto estructurado de datos personales accesibles con arreglo a criterios determinados y susceptibles de tratamiento para un fin específico, (…)

3. Principios del tratamiento

Los principios de protección de datos para realizar un tratamiento de datos personales son (…)

La aplicación de los principios del tratamiento contempla todas las operaciones realizadas sobre datos personales: 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.

4. Aplicación de la Responsabilidad proactiva

A continuación, se detallan las medidas aplicadas en cada fichero de datos para garantizar que se cumplen los principios del tratamiento.

Ejemplo

Ejemplos prácticos (política de información-I)

1. Identificación de la organización Responsable del tratamiento

De conformidad con lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril de 2016 (GDPR), la organización Responsable del tratamiento es quién determina los fines y los medios del tratamiento de datos personales (ficheros).

....

2. Identificación de los Ficheros de datos personales

...

3. Política de información y comunicación del tratamiento al interesado

El Responsable del tratamiento ha diseñado documentos concisos, transparentes, sencillos y accesibles para comunicar al interesado los detalles del tratamiento y el ejercicio de los derechos sobre sus datos…..

La información se facilitará al interesado de forma gratuita tanto si se refiere a la comunicación del tratamiento como a la solicitud de derechos.

La Organización ha implementado los siguientes protocolos de información y comunicación del tratamiento al interesado:

1. Transparencia y comunicación del tratamiento.
2. Información del tratamiento al interesado.
3. Comunicación de la información del tratamiento al interesado.
4. Ejercicio de los derechos del interesado

3.1. Transparencia y comunicación del tratamiento

Se facilitará por escrito o por medios electrónicos, u oralmente si lo solicita el interesado.

Ejemplo

Ejemplos prácticos (política de información-II)

3.2. Información del tratamiento al interesado

Se facilitará, como mínimo, la siguiente información (La base jurídica del tratamiento.

/ La identidad y los datos de contacto de la Organización Responsable del tratamiento./ Los fines específicos del tratamiento./ El plazo de conservación o los criterios que lo determinen….

Cuando existan casos específicos de tratamiento, además la siguiente información: (El interés legítimo del Responsable para realizar el tratamiento./ En elaboración automatizada de perfiles, la lógica aplicada y las consecuencias previstas para el interesado….)

Cuando los datos no se obtienen del interesado, además, se facilitará la siguiente información ..(Las categorías de datos tratados y su procedencia

3.3. Comunicación de la información del tratamiento al interesado

Cuando hayamos obtenido los datos directamente del interesado, se le comunicará la información….

Cuando no hayamos obtenido los datos del interesado, se le comunicará la información….

No será necesario que comuniquemos la información al interesado cuando:…

3.4. Ejercicio de los derechos del interesado

La Organización dispone de un protocolo de actuación para dar curso al ejercicio de l[illegible]derechos del interesado y ha diseñado una estructura técnico organizativa adecuada para que dicho protocolo sea efectivo.

4. Aplicación de la política de información

A continuación se detallan las medidas aplicadas en cada fichero de datos para garantizar la información del tratamiento.

- Normas
- Sanciones

Ejemplo

Ejemplos prácticos (obtención de consentimiento)

CONSENTIMIENTO PARA PERTENECER A LA LISTA DE DIFUSIÓN DE NOTICIAS

Conforme con lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril de 2016 relativo a la protección de datos personales, solicitamos su consentimiento para incluirle en la lista de difusión responsabilidad de ....., con el único fin de ....., por lo que se le facilita la siguiente información del tratamiento:

CRITERIOS DE CONSERVACIÓN DE LOS DATOS: se conservarán mientras exista un interés mutuo para mantener el fin del tratamiento y cuando ya no sea necesario para tal fin, se suprimirán con medidas de seguridad adecuadas para garantizar la seudonimización de los datos o la destrucción total de los mismos.

COMUNICACIÓN DE LOS DATOS: no se comunicarán los datos a terceros, salvo obligación legal.

DERECHOS DEL USUARIO: Podrá retirar este consentimiento en cualquier momento enviando un mensaje con la palabra BAJA. También podrá ejercer los derechos de acceso, rectificación, portabilidad, supresión, limitación y oposición que prevé el Reglamento comunicándolo al responsable del tratamiento mediante un mensaje por el mismo medio que recibe las comunicaciones. En todo caso, si considerase que el tratamiento de datos no se ajusta a la normativa vigente, siempre podrá presentar una reclamación ante la autoridad de control en www.agpd.es. [[DatosDPO]]

Si consiente el tratamiento de sus datos en los términos expuestos debe contestar este mensaje con el texto: SÍ ACEPTO

Ejemplo

Ejemplos prácticos (procedimientos de actuación ante el ejercicio de derechos)

Los interesados tendrán derecho a ser informados del tratamiento de sus datos personales y a obtener del RT el gobierno de los mismos, siempre que lo permita la legislación vigente.

Recepción de solicitudes

Registrar las solicitudes recibidas.
Identificar el interesado de manera inequívoca.
Comprobar que la solicitud se ajusta al GDPR.
Comprobar que el derecho no afecte negativamente los derechos y libertades de terceros.
Responder sin demora injustificada, como máximo en el plazo de 1 mes:

Atendiendo los derechos: comunicar la información del tratamiento.

Prorrogando la atención: comunicar los motivos del retraso (máximo 2 meses para casos complejos).

No atendiendo los derechos: razonar los motivos e informando del derecho a presentar una reclamación a la AC y de ejercitar acciones judiciales.

Atención de los derechos

Forma de facilitar la información:

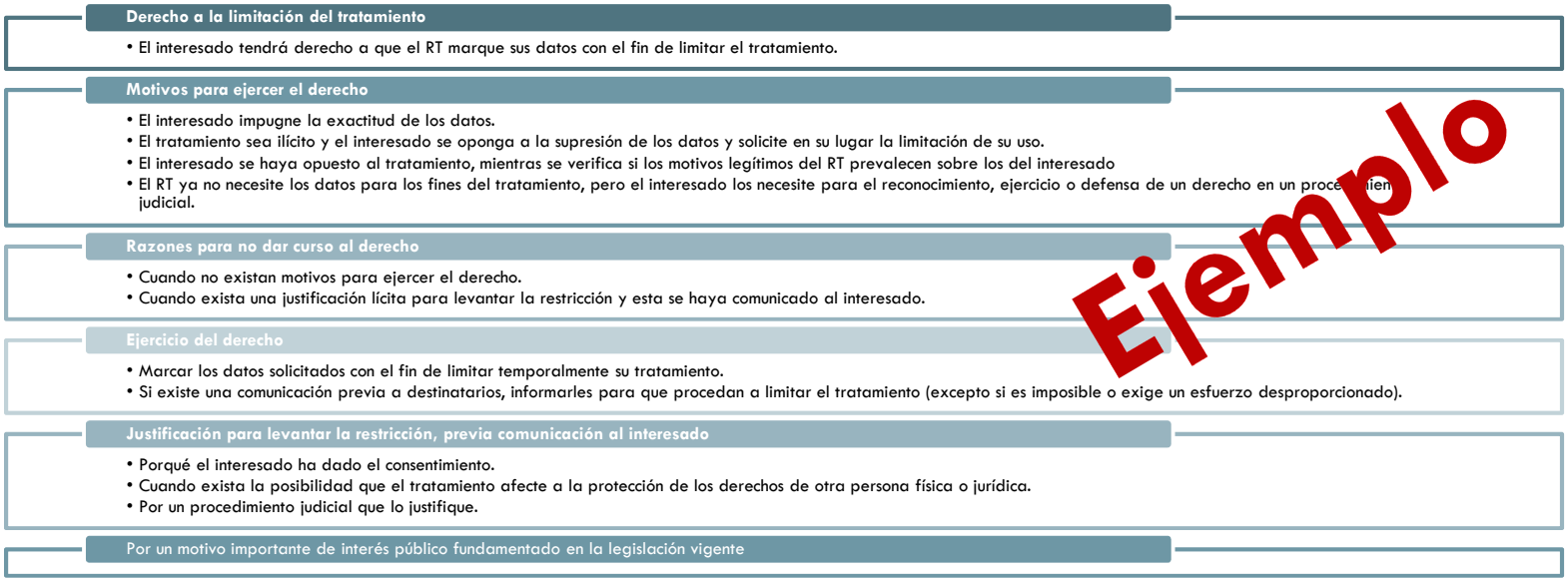
- Concisa, transparente, inteligible y de fácil acceso.
- Lenguaje claro y sencillo

Medios para facilitar la información:

- Por escrito.
- Medios electrónicos (obligatorio si se solicita por este medio).

Ejemplo

Ejemplos prácticos (procedimientos de actuación ante el ejercicio de derechos)



Recursos, responsabilidad y sanciones

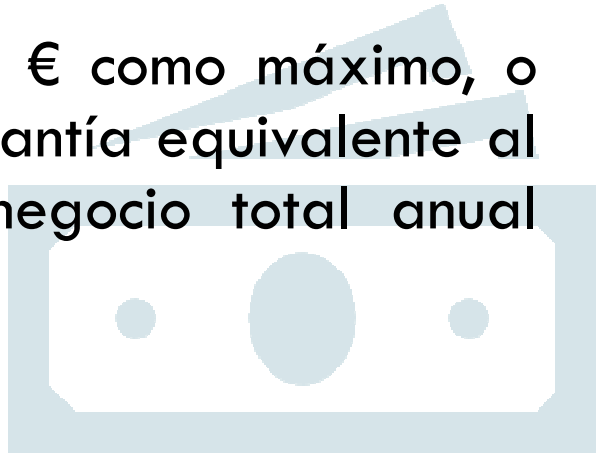
Recursos, responsabilidad y sanciones

En función de las circunstancias de cada caso individual, teniendo en cuenta:

- Naturaleza, gravedad, duración, intencionalidad, medidas tomadas, grado de responsabilidad, grado de cooperación con la autoridad de control, categorías de datos afectados, etc.
- Incumplimiento negligente: máximo multa más grave

Recursos, responsabilidad y sanciones

- Multas administrativas de 10.000.000 € como máximo, o tratándose de una empresa, de una cuantía equivalente al 2%como máximo del volumen de negocio total anual global del ejercicio financiero anterior
- Multas administrativas de 20.000.000 € como máximo, o tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior



Documentos de interés

- Guía del Reglamento para responsables del tratamiento
- Guía para el cumplimiento del deber de información
- Directrices para la elaboración de contratos
- Guía práctica de análisis de riesgos
- Guía práctica de evaluaciones de impacto
- Listado de cumplimiento normativo

Muchas gracias