



www.planalfa.es



www.integratics.com

Reglamento General de Protección de Datos Adaptación a la Nueva Normativa



Reglamento General de Protección de Datos

Introducción

- ❖ **Entró en vigor en mayo de 2016 y aplicable a partir de mayo de 2018**
- ❖ **Norma directamente aplicable, no requiere normas de trasposición**
- ❖ **La ley que sustituye a la actual Ley Orgánica de LOPD si podrá incluir precisiones.**
 - Las empresas que ya cumplen con la actual LOPD tienen una buena base de cumplimiento, pero es necesario adaptarse
- ❖ **Elementos de carácter general que las diferencia:**
 - **Principio de Responsabilidad Proactiva:** (necesidad de aplicación de medidas de seguridad y organizativas) Qué datos tratan, con qué finalidad, que operaciones de tratamiento realizan. Actitud consciente, diligente y proactiva.
 - **Enfoque de riesgo:** Las medidas deben tener en cuenta la naturaleza, el ámbito, el contexto, los fines del tratamiento así como el riesgo para los derechos y libertades de los afectados. Las medidas deben adaptarse a las características de las organizaciones

Base de legitimación para el tratamiento de datos

Todo tratamiento necesita legitimación

❖ Tipos de legitimidad

- Consentimiento
- Relación contractual
- Intereses vitales del interesado o de otras personas
- Obligación legal para el responsable
- Interés público o ejercicio de poderes públicos



❖ Obligaciones

- Identificar e Incluir la base legal en la información a la hora de recoger los datos
- Documentar los intereses legítimos en los que se fundamentan las operaciones de tratamiento
- Uno y otro debe adaptarse al tipo de tratamiento y a las características de las organizaciones

Base de legitimación para el tratamiento de datos

Consentimiento

❖ Inequívoco

- Manifestación del Interesado mediante una clara acción afirmativa

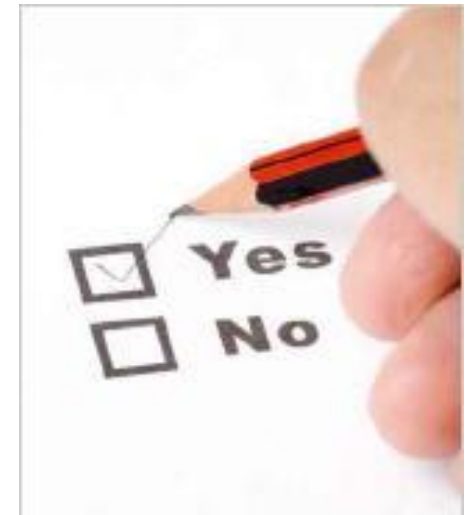
❖ Explícito

- Tratamiento de datos sensibles
- Adopción de decisiones automatizadas
- Transferencias internacionales

❖ Verificable

❖ Obligaciones

- Obtención de un consentimiento válido
- Valorar si los tratamientos afectados pueden apoyarse en otra base legal
- Necesidad de revisar consentimientos tácitos o por omisión



Base de legitimación para el tratamiento de datos

Transparencia e información

❖ Información

- Concisa
- Transparente
- Inteligible
- Fácil acceso
- Lenguaje claro y sencillo

❖ Obligaciones

- Evitar fórmulas farragosas y que incorporan remisiones a textos legales
- Explicar el contenido con independencia de su conocimiento en la materia
- Necesidad de revisar consentimientos tácitos o por omisión
- Debe contener: Base jurídica del tratamiento, Intención de realizar transferencias internacionales, datos del Delegado de protección de datos (si lo hubiera) y Elaboración de perfiles



Derechos

Cómo se garantiza el ejercicio de los derechos de los afectados

❖ Gratuito, accesible y sencillo (un mes)

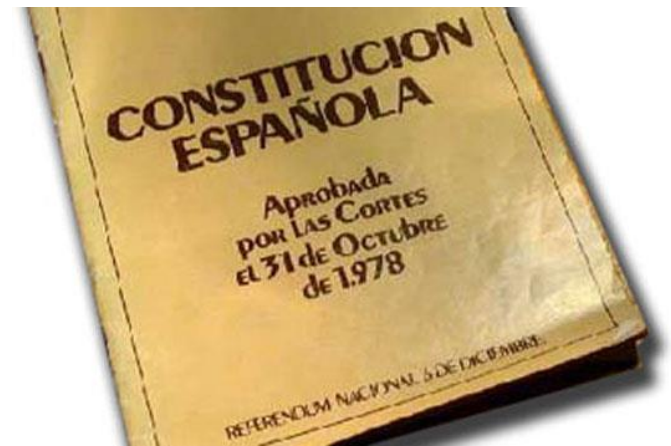
- Habilitar que los interesados puedan ejercer su derecho por medios electrónicos, especialmente si el tratamiento se realiza por dichos medios.

❖ Derechos ARCO

- Acceso
- Rectificación
- Cancelación
- Oposición

❖ Nuevos derechos

- Derecho al olvido (manifestación del derecho de cancelación)
- Limitación del tratamiento (Ilícito pero el afectado se opone o ejercicio de derechos)
- Portabilidad (Formato estructurado, de uso común y lectura mecánica)



Relaciones Responsable-Encargado

Obligaciones expresas para los Encargados del Tratamiento

- ❖ **Los encargados del tratamiento están obligados a:**
 - Registro de actividades del tratamiento
 - Determinar las medidas de seguridad aplicables
 - Designar un Delegado de Protección de Datos

- ❖ **El Responsable del tratamiento debe exigir garantías de que el encargado puede realizar el tratamiento conforme al RGPD**

- ❖ **Contrato de Encargo (adaptación)**
 - Objeto duración, naturaleza y finalidad de los tratamientos.
 - Tipo de datos personales y categorías de interesados
 - Obligación del tratamiento conforme a instrucciones
 - Condiciones para que el responsable consienta subcontrataciones
 - Asistencia al responsable en caso de ejercicio de derechos



Medidas de Responsabilidad Activa

1. Análisis de Riesgo

- ❖ **El establecimiento de medidas de seguridad del responsable y el encargado está condicionado a la evaluación del riesgo. El análisis variará en función de:**
 - Los tipos de tratamiento
 - Naturaleza de los datos
 - Número de afectados
 - Cantidad y variedad de tratamientos

- ❖ **En grandes organizaciones debe aplicarse una metodología de análisis de riesgo existentes**

- ❖ **En pequeñas organizaciones el análisis será el resultado de una reflexión documentada sobre las implicaciones de los tratamientos en los derechos y libertades de los afectados**



Medidas de Responsabilidad Activa

1. Análisis del Riesgo: Medición

❖ Si es afirmativas todas o algunas de las siguientes reflexiones deben considerarse la necesidad de una **Evaluación de Riesgos de Protección de Datos (EIPD)**

- ¿Se tratan datos sensibles o de menores?
- ¿Se incluyen datos de una gran cantidad de personas?
- ¿Se elaboran perfiles de comportamiento?
- ¿Se cruzan datos aportados por los interesados con otros de otras fuentes?
- ¿Se van a utilizar para una finalidad distinta?
- ¿Hay técnicas de análisis tipo Big Data?
- ¿Se utilizan tecnología invasivas para la privacidad tipo geolocalización, video-vigilancia o aplicaciones de Internet de las cosas?



Medidas de Responsabilidad Activa

2. Registro de actividades de tratamiento

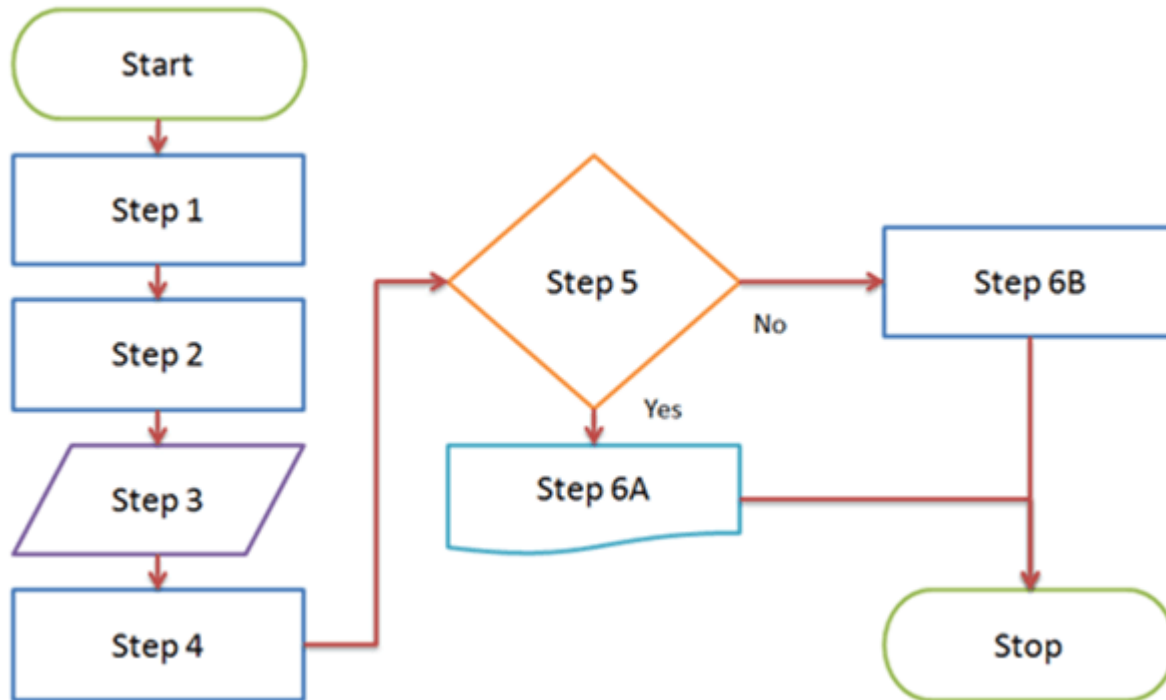
- ❖ **Debe existir por parte del responsable y por parte del encargado un registro de operaciones de tratamiento que incluya**
 - Más de 250 empleados o tratamientos de alto riesgo
 - Contacto del responsable y encargado en su caso
 - Finalidades del tratamiento
 - Categorías de interesados y de datos personales tratados
 - Transferencias Internacionales de datos
- ❖ **En el registro de la AEPD se puede detallar las operaciones que se realizan sobre cada fichero**



Medidas de Responsabilidad Activa

3. Protección de datos desde el diseño por defecto

- ❖ Se trata de pensar en términos de protección de datos desde el mismo momento en que se diseña un tratamiento



Medidas de Responsabilidad Activa

4. Medidas de seguridad

- ❖ **Antes las medidas de seguridad estaban basadas en el tipo de datos, ahora se toman en consideración más variables:**
 - Coste de la técnica
 - Costes de la aplicación
 - Naturaleza, alcance, contexto y fines del tratamiento
 - Riesgos para los derechos y libertades

- ❖ **El esquema de medidas de seguridad según tipo de datos no será válido a partir de ahora**

- ❖ **Necesidad de análisis del riesgo**



Medidas de Responsabilidad Activa

5. Notificación de Violaciones de Seguridad de los Datos

❖ **Cualquier quiebra de seguridad que ocasione:**

- Destrucción, pérdida o alteración accidental o ilícita de datos personales, transmitidos, conservados o tratados
- Comunicación o acceso no autorizado

❖ **Debe documentarse siempre y notificarse a la autoridad competente (AEPD) en 72 h., a menos que sea improbable que suponga un riesgo para los derechos y libertades de los afectados. Debe incluir:**

- Naturaleza de la violación
- Categoría de datos y de afectados
- Medidas de seguridad adoptadas por el responsable para solventar la quiebra
- Medidas para paliar los efectos negativos para los interesados

❖ **Comunicación sin dilación, a los afectados, si entraña alto riesgo para los derechos o libertades de los interesados: contraseñas, participación en determinadas actividades, o posibles perjuicios económicos o morales**



Medidas de Responsabilidad Activa

6. Evaluación del Impacto sobre la Protección de Datos (EIPD)

- ❖ **Existe un contenido mínimo de las Evaluaciones**

- ❖ **Con carácter previo a tratamientos de alto riesgo**
 - Elaboración de perfiles que produzcan efectos jurídicos
 - Tratamiento a **gran escala** de datos sensibles
 - Número de personas afectadas
 - Volumen y variedad de datos
 - Duración o permanencia del tratamiento
 - Extensión geográfica de la actividad del tratamiento
 - Observación sistemática a gran escala de una zona de acceso público

- ❖ **AEPD podrá elaborar listados de tratamientos que requieran EIPD así como tratamientos en los que no.**



Medidas de Responsabilidad Activa

7. Delegado de Protección de Datos

❖ Obligatorio para

- Autoridades y organismos públicos
- Tratamientos que requieran una observación habitual y sistemática de interesados a gran escala
- Tratamiento a gran escala con datos sensibles o datos relativos a condenas e infracciones penales

❖ Atendiendo a su cualificación profesional y conocimiento de la legislación y la práctica de la protección de datos

❖ Debe ser comunicada a la AEPD

❖ Requisitos

- Autonomía en el ejercicio de sus funciones
- Debe relacionarse con el nivel superior de la dirección
- Debe proporcionársele todos los medios necesarios
- Certificación por parte de la AEPD



Transferencias Internacionales

Comunicaciones fuera del Espacio Económico Europeo

❖ Solo podrán comunicarse:

- A países y territorios, sectores específicos u organizaciones sobre las que la comisión reconoce que ofrece un nivel de protección adecuado
- Cuando se ofrecen garantías adecuadas en el destino
- O que sea una excepción por razones de seguridad o interés general

❖ Se reconocen las decisiones anteriores de la AEPD:

- Adecuación
- Cláusulas tipo
- Autorizaciones de transferencia
- Garantías
- Normas corporativas vinculantes, cláusulas contractuales estándar y certificaciones no necesitan autorización AEPD



Adaptándose a los cambios

Plan de Acción

- ❖ Comprobación de legitimidad del tratamiento
- ❖ Adecuación de las cláusulas de información
- ❖ Adecuación de cláusulas de consentimiento
- ❖ Adecuación contratos con Encargados del tratamiento
- ❖ Registro de las actividades de tratamiento
- ❖ Protocolo de notificaciones de violaciones de seguridad
- ❖ Nombramiento de Delegado de Protección de Datos (DPD)
- ❖ Evaluación de Impacto de Protección de Datos (EIPD)
- ❖ Establecimiento de medidas de seguridad (Salvaguardas)



Plan de
Acción

Integra Información y Comunicación S.L.

Twitter: @GDCS_

Web: www.grupodcsolutions.com

Blog: <https://www.grupodcsolutions.com/blog>



❖ Más información:

- 917454270
- proxi@planalfa.es
- www.planalfa.es

