Legislación y jurisprudencia en materia de protección de datos (Normativa de ciberseguridad)

Principios de protección de datos

El Reglamento General de Protección de Datos señala un conjunto de principios que los responsables y encargados del tratamiento deben observar al tratar datos personales (fuente de la información AEPD):

- Principio de " licitud, transparencia y lealtad", que consiste en que los datos deben ser tratados de manera lícita, leal y transparente para el interesado.
- Principio de " limitación de la finalidad" que implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.
- Principio de " minimización de datos", es decir, que los datos sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- Los datos, según el "principio de exactitud", deben ser exactos y, si fuera preciso, actualizados, debiendo adoptarse todas las medidas razonables para que se rectifiquen o supriman los datos inexactos en relación a los fines que se persiguen.
- El principio de " limitación del plazo de conservación" está relacionado con el de minimización. Igual que solo

pueden tratarse los datos adecuados, pertinentes y necesarios para una finalidad, la conservación de esos datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados.

- Principio de "integridad y confidencialidad". Básicamente, impone a quienes tratan datos la obligación de actuar proactivamente con el objetivo de proteger los datos que manejan frente a cualquier riesgo que amenace su seguridad.

Además, se encuentra el principio denominado de" responsabilidad proactiva", expresión que pretende traducir el término inglés " accountability", según el cual los responsables aplicarán las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el Reglamento.

Novedades del RGPD de la Unión Europea

Reglamento (UE) 2016/679 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 (este texto incluye la corrección de errores publicada en el DOUE de 23 de mayo de 2018).

El Reglamento es una medida esencial para fortalecer los derechos fundamentales de las personas en la era digital y facilitar la actividad económica, ya que aclara las normas aplicables a las empresas y los organismos públicos en el mercado único digital. Además, la existencia de una norma única pone fin a la fragmentación en distintos sistemas nacionales y a las cargas administrativas innecesarias.

El Reglamento, que entró en vigor el 24 de mayo de 2016, se aplica desde el 25 de mayo de 2018. Más información para particulares y empresas.

Información sobre la incorporación del Reglamento General de Protección de Datos (RGPD) al Acuerdo EEE.

EU Member States notifications to the European Commission under the GDPR

Study on Data Protection Certification Mechanisms

Directiva (UE) 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos.

La Directiva protege el derecho fundamental de los ciudadanos a la protección de sus datos cuando los utilicen las autoridades policiales y judiciales a efectos de aplicación de la ley. Más concretamente, la Directiva garantizará que se protejan adecuadamente los datos personales de víctimas, testigos y sospechosos de delitos, además de facilitar la cooperación transfronteriza en la lucha contra la delincuencia y el terrorismo.

La Directiva entró en vigor el 5 de mayo de 2016, y los países de la UE debían incorporarla a su legislación nacional no más tarde del 6 de mayo de 2018.

Privacidad por Diseño y por Defecto

En el RGPD se hace referencia a dos principios para la implementación efectiva de la responsabilidad proactiva como son los de protección de datos desde el diseño y protección de datos por defecto (fuente de la información AEPD).

El principio de **protección de datos desde el diseño** tiene como objetivo cumplir los requisitos definidos en el RGPD y, por tanto, los derechos de los interesados y busca que la protección de datos se encuentre presente en las primeras fases de concepción de un proyecto.

Estos requisitos se van a traducir en medidas técnicas y organizativas con el objeto de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento.

Un ejemplo de dichas medidas, que se establece de forma expresa en el RGPD, es que el propio tratamiento incorpore medidas para la minimización de datos, así como la **seudoanonimización** temprana de los datos personales, es decir, el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional.

En el caso de adquisición de productos o contratación de servicios que sean utilizados para la implementación de un tratamiento, entre los elementos que se utilizarán para determinación de la elección entre los disponibles en el mercado ha de figurar, con un peso significativo, el hecho de que se pueda demostrar que en su desarrollo se han implementado los principios de privacidad desde el diseño.

La obligación de que se adopten los principios de privacidad desde el diseño recae en el responsable del tratamiento. Sea cual sea la forma de subcontratación o adquisición, el responsable nunca podrá delegar completamente sus obligaciones de aplicación de este principio, ya que siempre quedará bajo su poder de decisión al menos aquellas medidas organizativas que le compete tomar para interaccionar con el servicio subcontratado.

El concepto de **privacidad por defecto** se refiere a que sólo sean objeto de tratamiento los datos personales que sean

estrictamente necesarios para cada uno de los fines de tratamiento. Es decir, independientemente del conjunto de datos recogidos por el responsable con el objeto de implementar los distintos servicios que se proporcionan al sujeto de los datos, el responsable ha de compartimentar el uso del conjunto de datos entre los distintos tratamientos, de tal forma que no todos los tratamientos accedan a todos los datos, sino que actúen solo sobre aquellos que sean necesarios y en los momentos en que sea estrictamente necesario.

El principio de « *necesidad de conocer*» se aplica a la protección de datos de carácter personal en la medida que significa que los empleados de la empresa sólo han de tener acceso a los datos de carácter personal que son estrictamente necesarios para realizar su trabajo o proporcionar un servicio.

Posibles estrategias básicas que permiten implementar la privacidad por defecto:

- Recogida de datos: analizar los tipos de datos que se recaban con un criterio de minimización en función de los productos y servicios seleccionados por el usuario;
- Tratamiento de los datos: analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos;
- Conservación: implementar una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios;
- Accesibilidad: limitar el acceso por parte de terceros a dichos datos personales.

Como en el caso de la privacidad desde el diseño, estos requisitos se van a traducir en medidas tanto técnicas como organizativas.

Análisis de Impacto en Privacidad (PIA), y medidas de seguridad

El Reglamento General de Protección de Datos (RGPD) introduce el concepto de Evaluación de Impacto relativa a la Protección de Datos (EIPD) en su artículo 35.

Una EIPD es un proceso ligado a los **principios de protección de datos desde el diseño y protección de datos por defecto** concebido para describir, de **manera anticipada y preventiva**, un tratamiento de datos personales, evaluar su necesidad y proporcionalidad y gestionar los potenciales riesgos para los derechos y libertades a los que estarán expuestos los datos personales en función de las actividades de tratamiento que se lleven a cabo con los mismos, determinando las medidas necesarias para reducirlos hasta un nivel de riesgo aceptable.

Esta obligación debe entenderse en el contexto de la responsabilidad proactiva y la obligación general de gestionar adecuadamente los riesgos y demostrar que se han tomado las medidas adecuadas para garantizar el cumplimiento de los requisitos exigidos por el RGPD.

La AEPD ha elaborado una guía para la Evaluación de Impacto en la Protección de los Datos Personales con el objetivo de promover una cultura proactiva de la privacidad y ofrecer directrices y orientaciones de cómo definir y establecer una metodología para la realización de una EIPD, sin perjuicio de que, aquellas organizaciones que tengan ya implantados procesos y herramientas de análisis de riesgos pueden utilizarlas para evaluar los relativos a la privacidad y la protección de datos, siempre que cubran los aspectos esenciales que toda Evaluación de Impacto en la Protección de Datos debe tener, respetando los requerimientos del RGPD.

Delegado de Protección de Datos (DPO)

El Delegado de Protección de Datos asegura, de manera independiente, que una organización aplica las leyes que protegen los datos personales de las personas.