Bigastro
Ayuntamiento

Taller sobre cumplimiento de Protección de Datos

CICLO DE ACTIVIDADES «BIGASTRO CRECE» 2023

CONTENIDO

Presentación teórica:

-Contexto: normas y AEPD

-Conceptos, principios y licitud

-Derechos

-Medidas

Parte práctica:

-Ejercicio de derechos y autoevaluación del cumplimiento

-Herramienta para la adecuación

CONTEXTO: NORMAS

-Art. 18.4 de la Constitución Española (1978)

-Convenio n.º 108 del Consejo de Europa (1981)

-Ley Orgánica 5/1992 (LOPD) y Directiva europea de 1995

-Carta de los Derechos Fundamentales de la Unión Europa (2000)

-Sentencia del Tribunal Constitucional 292/2000

-Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo 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 (**RGPD**, 2018)

-Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (**LOPDGDD**)

CONTEXTO: AEPD

CONCEPTOS

datos personales: toda información sobre una persona física identificada o identificable (el **interesado**); 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;

tratamiento: 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;

CONCEPTOS

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

CONCEPTOS

tercero: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado

destinatario: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento

CONCEPTOS

cesión de datos: toda comunicación por transmisión y/o difusión de datos de carácter personal que se realiza a un tercero, bien sea persona física o jurídica, pública o privada, autoridad pública, servicio u organismo

brecha de seguridad: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos

PRINCIPIOS (ART. 5 RGPD)

-Licitud, transparencia y lealtad: los datos deben ser tratados de manera lícita, leal y transparente para el interesado.

-Finalidad: 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.

-Minimización de datos: serán objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento reduciendo, la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad.

-Exactitud: disponer de medidas razonables para que los datos se encuentren actualizados, se supriman o modifiquen sin dilación cuando sean inexactos con respecto a los fines para los que se tratan.

PRINCIPIOS (ART. 5 RGPD)

-Limitación del plazo de conservación: la conservación debe limitarse en el tiempo al logro de los fines que persigue el tratamiento. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados, bloqueados o, en su defecto, anonimizados, es decir, desprovistos de todo elemento que permita identificar a los interesados.

-Seguridad: que impone a quienes tratan datos el necesario análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten.

-Responsabilidad activa o responsabilidad demostrada: obliga a los responsables a mantener diligencia debida de manera de modo que pueda tanto garantizar como estar en condiciones de demostrar que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGD.

Ejemplos de incumplimiento

NOTICIAS JURÍDICAS

2.000 € de multa por solicitar el número de teléfono a una clienta para emitir una factura

Según la AEPD, pedir el dato del número de teléfono "resulta excesivo" para el fin que se perseguía

> La Agencia Española de Protección de Datos impone una sanción de 60.000 euros a una empresa comercializadora de gas y electricidad por una infracción del artículo 5.1 del Reglamento General de Protección de Datos.

BASES LICITUD (ART. 6 RGPD)

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su **consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un **contrato** en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una **obligación legal** aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger **intereses** vitales del **interesado** o de **otra persona física**;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en **interés público** o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de **intereses** legítimos perseguidos por el **responsable del tratamiento o por un tercero**, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

CONDICIONES CONSENTIMIENTO (ART. 7 RGPD)

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de **demostrar** que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de **forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo**. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá **derecho a retirar su consentimiento** en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha **dado libremente**, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

CATEGORÍAS ESPECIALES DE DATOS (ART. 9 RGPD)

1. Quedan prohibidos el tratamiento 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**.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su **consentimiento explícito** para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el **ámbito del Derecho laboral y de la seguridad y protección social**, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

DEBER DE INFORMACIÓN (ART. 13)

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

Artículo 14 *Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado*

1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:

(…)

1.ª Capa: Información básica (resumida)

-La identidad del responsable del tratamiento

-Una descripción sencilla de los fines del tratamiento, incluyendo la elaboración de perfiles si existiese

-La base jurídica del tratamiento

-Previsión o no de cesiones.

-Previsión o no de transferencias a terceros países

-Referencia al ejercicio de derechos

2.ªCapa: Información adicional (detallada)

-Datos de contacto del responsable.

-Identidad y datos del representante (si existiese).

-Datos de contacto del delegado de protección de datos (si existiese).

-Descripción ampliada de los fines del tratamiento.

-Plazos o criterios de conservación de los datos. Decisiones automatizadas, perfiles y lógica aplicada.

-Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo.

-Obligación o no de facilitar datos y consecuencias de no hacerlo.

-Destinatarios o categorías de destinatarios.

-Decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables.

-Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de los datos, y la limitación u oposición a su tratamiento.

-Derecho a retirar el consentimiento prestado. Derecho a reclamar ante la Autoridad de Control.

DERECHOS (CAPÍTULO III RGPD)

-Derecho de acceso

-Derecho de rectificación

-Derecho de oposición

-Derecho de supresión ("al olvido")

-Derecho a la limitación del tratamiento

-Derecho a la portabilidad

-Derecho a no ser objeto de decisiones individuales automatizadas

MEDIDAS DE SEGURIDAD (ART. 32 RGPD)

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, **el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo**, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

OTRAS POSIBLES OBLIGACIONES

-Gestión de brechas de datos personales

-Elaboración de un Registro de Actividades de Tratamiento

-Designación de Delegado de Protección de Datos

-Análisis de Riesgos y Evaluación de impactos

PRIMEROS PASOS: HERRAMIENTA AEPD