Curso introductorio a la normativa de Protección de Datos (RGPD - LOPDGDD)

visual

Principios relativos al Tratamiento de los Datos Personales

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 “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”
Aplicar medidas técnicas y organizativas para garantizar que sean 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.

Principio de “exactitud”
Que obliga a los responsables a 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.

Principio de “limitación del plazo de conservación”
Que constituye una de las materializaciones del principio de minimización. La conservación de esos datos 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.

Principio de “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.

Principio de “responsabilidad activa” o “responsabilidad demostrada”
Que obliga a los responsables a mantener diligencia debida de manera permanente para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados en base a un análisis de los riesgos que el tratamiento representa para esos derechos y libertades, de modo que el responsable pueda, tanto garantizar como estar en condiciones de demostrar que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGD.

EL DEBER DE INFORMAR. CONCEPTOS CLAVE

epígrafe	información básica (1ª capa, resumida)	información adicional (2ª capa, detallada)
RESPONSABLE *(del tratamiento)*	Identidad del responsable del tratamiento	Datos de contacto del Responsable Identidad y datos de contacto del Representante Datos de contacto del Delegado de Protección de Ddatos
FINALIDAD *(del tratamiento)*	Descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles	Descripción ampliada de los fines del tratamiento Plazos o criterios de conservación de los datos Decisiones automatizadas, perfiles y lógica ampliada
LEGITIMACIÓN *(del tratamiento)*	Base jurídica del tratamiento	Detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo Obligación o no de faciliatr datos y consecuencia de no hacerlo
DESTINATARIOS *(de cesiones o transferencias)*	Previsión o no de Cesiones Previsión de Transferencias , o no, a terceros paises	Destinatarios o categorías de destinatarios Decisiones de adecuación, garantías, normas corproativas vinculantes o situaciones específicas aplicables
DERECHOS *(de las personas interesadas)*	Referencia al ejercicio de derechos	Cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos y lalimitación u oposición al tratamiento, Derecho a retirar el consentimiento prestado Derecho a reclamar ante la Autoridad de Control
PROCEDENCIA *(de los datos)*	Fuente de los datos (cuando no proceden de interesado)	Información detallada del origen de los datos, incluso si proceden de fuentes de acceso público Categorías de datos que se traten

Condiciones para el consentimiento

CARGA DE LA PRUEBA DEL CONSENTIMIENTO

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.
Por tanto, el responsable del tratamiento debe de guardar prueba de que dicho interesado ha prestado de una forma efectiva dicho consentimiento.

DERECHO A RETIRAR SU CONSENTIMIENTO

Es importante destacar que el interesado siempre va a tener **derecho a retirar su consentimiento** en cualquier momento.
La presente acción, en ningún caso, va a afectar a la licitud del tratamiento basada en el consentimiento previo a su retirada.

CONSENTIMIENTO LIBREMENTE PRESTADO

El consentimiento no debe considerarse **libremente prestado** cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno

DERECHOS DEL INTERESADO

LOS DERECHOS QUE TIENES PARA PROTEGER TUS DATOS PERSONALES

EL 25 DE MAYO DE 2018 SE APLICA EL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS Y ES IMPORTANTE QUE CONOZCAS CUÁLES SON TUS DERECHOS

1 DERECHO A CONOCER

- PARA QUÉ UTILIZAN TUS DATOS
  - Quién los tiene
  - Para qué los tienen
  - A quién los pueden ceder
  - Quiénes son sus destinatarios
- EL PLAZO DE CONSERVACIÓN DE TUS DATOS o Hasta cuándo van a ser utilizados
- QUE PUEDES PRESENTAR UNA RECLAMACIÓN ANTE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
- LA EXISTENCIA DE DECISIONES AUTOMATIZADAS, LA ELABORACIÓN DE PERFILES Y SUS CONSECUENCIAS

2 DERECHO A SOLICITAR AL RESPONSABLE

- LA SUSPENSIÓN DEL TRATAMIENTO DE TUS DATOS
  - Si impugnamos la exactitud de los datos, mientras se verifica dicha exactitud por parte del responsable
  - Si hemos ejercitado nuestro derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre tus derechos
- LA CONSERVACIÓN DE TUS DATOS
  - Si el tratamiento es ilícito y nos oponemos a la supresión de los datos solicitando la limitación de su uso
  - Si los datos se necesitan para la formulación, ejercicio o defensa de reclamaciones
- LA PORTABILIDAD DE TUS DATOS A OTROS PROVEEDORES DE SERVICIOS
  - En un formato estructurado, de uso común y lectura mecánica, siempre que sea técnicamente posible para su portabilidad y cuando los hayan utilizado/tratado con tu consentimiento o por existir un contrato

3 DERECHO A RECTIFICAR TUS DATOS

- CUANDO SEAN INEXACTOS
- CUANDO ESTÉN INCOMPLETOS

4 DERECHO A SUPRIMIR TUS DATOS

- POR TRATAMIENTO ILÍCITO DE DATOS
- POR LA DESAPARICIÓN DE LA FINALIDAD QUE MOTIVÓ EL TRATAMIENTO O RECOGIDA
- CUANDO REVOCAS TU CONSENTIMIENTO
- CUANDO TE OPONES A QUE SE TRATEN

5 DERECHO DE OPOSICIÓN AL TRATAMIENTO DE TUS DATOS

- POR MOTIVOS PERSONALES SALVO QUE QUIEN TRATA TUS DATOS ACREDITE UN INTERÉS LEGÍTIMO
- CUANDO EL TRATAMIENTO TENGA POR OBJETO EL MARKETING DIRECTO

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

www.agpd.es

visual academy

SEGURIDAD

Tablas medidas de seguridad

CUADRO RESUMEN

	Nivel Básico	Nivel Medio	Nivel Alto
RESPONSABLE DE SEGURIDAD		El responsable del fichero tiene que designar a uno o varios responsables de seguridad (no es una delegación de responsabilidad). El responsable de seguridad es el encargado de coordinar y controlar las medidas del documento.	
PERSONAL	Funciones y obligaciones de los diferentes usuarios o de los perfiles de usuarios claramente definidas y documentadas. Definición de las funciones de control y las autorizaciones delegadas por el responsable. Difusión entre el personal, de las normas que les afecten y de las consecuencias por su incumplimiento.		
INCIDENCIAS	Registro de incidencias: tipo, momento de su detección, persona que la notifica, efectos y medidas correctoras. Procedimiento de notificación y gestión de las incidencias.	SOLO FICHEROS AUTOMATIZADOS Anotar los procedimientos de recuperación, persona que lo ejecuta, datos restaurados, y en su caso, datos grabados manualmente. Autorización del responsable del fichero para la recuperación de datos.	
CONTROL DE ACCESO	Relación actualizada de usuarios y accesos autorizados. Control de accesos permitidos a cada usuario según las funciones asignadas. Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. Concesión de permisos de acceso sólo por personal autorizado. Mismas condiciones para personal ajeno con acceso a los recursos de datos.	SOLO FICHEROS AUTOMATIZADOS Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información.	SOLO FICHEROS AUTOMATIZADOS Registro de accesos: usuario, hora, fichero, tipo de acceso, autorizado o denegado. Revisión mensual del registro por el responsable de seguridad. Conservación 2 años. No es necesario este registro si el responsable del fichero es una persona física y es el único usuario. SOLO FICHEROS NO AUTOMATIZADOS Control de accesos autorizados. Identificación accesos para documentos accesibles por múltiples usuarios.

Ver más info en :
https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf

Tablas medidas de seguridad

	Nivel Básico	Nivel Medio	Nivel Alto
IDENTIFICACIÓN Y AUTENTICACIÓN	SOLO FICHEROS AUTOMATIZADOS Identificación y autenticación personalizada. Procedimiento de asignación y distribución de contraseñas. Almacenamiento ininteligible de las contraseñas. Periodicidad del cambio de contraseñas (<1 año).	SOLO FICHEROS AUTOMATIZADOS Limite de intentos reiterados de acceso no autorizado.	
GESTIÓN DE SOPORTES	Inventario de soportes. Identificación del tipo de información que contienen, o sistema de etiquetado. Acceso restringido al lugar de almacenamiento. Autorización de las salidas de soportes (incluidas a través de e-mail) Medidas para el transporte y el desecho de soportes.	SOLO FICHEROS AUTOMATIZADOS Registro de entrada y salida de soportes: documento o soporte, fecha, emisor/destinatario, número, tipo de información, forma de envío, responsable autorizado para recepción/entrega.	SOLO FICHEROS AUTOMATIZADOS Sistema de etiquetado confidencial. Cifrado de datos en la distribución de soportes. Cifrado de información en dispositivos portátiles fuera de las instalaciones (evitar el uso de dispositivos que no permitan cifrado, o adoptar medidas alternativas).
COPIAS DE RESPALDO	SOLO FICHEROS AUTOMATIZADOS Copia de respaldo semanal. Procedimientos de generación de copias de respaldo y recuperación de datos. Verificación semestral de los procedimientos. Reconstrucción de los datos a partir de la última copia. Grabación manual en su caso, si existe documentación que lo permita. Pruebas con datos reales. Copia de seguridad y aplicación del nivel de seguridad correspondiente.		SOLO FICHEROS AUTOMATIZADOS Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
CRITERIOS DE ARCHIVO	SOLO FICHEROS NO AUTOMATIZADOS El archivo de los documentos debe realizarse según criterios que faciliten su consulta y localización para garantizar el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO)		

Ver más info en :
https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf

Tablas medidas de seguridad

	Nivel Básico	Nivel Medio	Nivel Alto
ALMACENAMIENTO	SOLO FICHEROS NO AUTOMATIZADOS Dispositivos de almacenamiento dotados de mecanismos que obstaculicen su apertura.		SOLO FICHEROS NO AUTOMATIZADOS Armarios, archivadores de documentos en áreas con acceso protegido mediante puertas con llave.
CUSTODIA SOPORTES	SOLO FICHEROS NO AUTOMATIZADOS Durante la revisión o tramitación de los documentos, la persona a cargo de los mismos debe ser diligente y custodiarla para evitar accesos no autorizados.		
COPIA O REPRODUCCIÓN			SOLO FICHEROS NO AUTOMATIZADOS Sólo puede realizarse por los usuarios autorizados. Destrucción de copias desechadas.
AUDITORIA		Al menos cada dos años, interna o externa. Debe realizarse ante modificaciones sustanciales en los sistemas de información con repercusiones en seguridad. Verificación y control de la adecuación de las medidas. Informe de detección de deficiencias y propuestas correctoras. Análisis del responsable de seguridad y conclusiones elevadas al responsable del fichero.	
TELECOMUNICACIONES			SOLO FICHEROS AUTOMATIZADOS Transmisión de datos a través de redes electrónicas cifradas.
TRASLADO DOCUMENTACIÓN			SOLO FICHEROS NO AUTOMATIZADOS Medidas que impidan el acceso o manipulación.

Ver más info en :
https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf

visual

visualnacert.com