DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 15| Septiembre 2021

LA PROTECCIÓN DE LOS DATOS PERSONALES EN SOPORTE PAPEL

Í N D I C E

LA PROTECCIÓN DE LOS DATOS PERSONALES EN SOPORTE PAPEL

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

Si bien en los últimos años se ha producido un impulso en la adopción de procesos y medios digitales en la Administración Pública, avanzando en la digitalización de la gestión de los servicios públicos, lo cierto es que el papel aún ocupa un lugar importante en nuestro día a día.

Al tratamiento no automatizado de datos personales, como el que se realiza con los documentos en soporte papel, también le es de aplicación la normativa de protección de datos, por lo que han de adoptarse las medidas oportunas para garantizar un nivel de seguridad adecuado.

No obstante, es habitual que los documentos en papel que contienen datos personales terminen en armarios, cajones o mesas, sin ningún tipo de medida de seguridad. Por eso, es fundamental que todos los usuarios de los sistemas de información de la Diputación de Valencia que, para la realización de sus funciones y tareas, accedan o traten información de carácter personal en soporte papel, conozcan las medidas que deben adoptar.

La aplicación de estas medidas, junto a un adecuado plan de formación y concienciación del personal, nos ayudará a proteger de manera adecuada nuestra organización.

"ES HABITUAL QUE LOS DOCUMENTOS EN PAPEL QUE CONTIENEN DATOS PERSONALES TERMINEN EN ARMARIOS, CAJONES O MESAS, SIN NINGÚN TIPO DE MEDIDA DE SEGURIDAD. ES FUNDAMENTAL QUE TODOS LOS USUARIOS DE LOS SISTEMAS DE INFORMACIÓN DE LA DIPUTACIÓN DE VALENCIA QUE ACCEDAN O TRATEN INFORMACIÓN DE CARÁCTER PERSONAL EN PAPEL PARA LA REALIZACIÓN DE SUS FUNCIONES Y TAREAS, APLIQUEN LAS MEDIDAS OPORTUNAS PARA GARANTIZAR UN NIVEL DE SEGURIDAD ADECUADO".

¿QUÉ MEDIDAS DEBEMOS ADOPTAR PARA PROTEGER LOS DATOS PERSONALES EN SOPORTE PAPEL?

En relación con los ficheros en soporte papel, debes adoptar las siguientes medidas:

Cierre de despachos o dependencias. – En caso de disponer de un despacho o dependencia donde se almacenen documentos con datos personales, debes asegurarte de que la puerta se cierra con llave al término de la jornada laboral o cuando te ausentes temporalmente de esta ubicación, a fin de evitar accesos no autorizados.

Custodia de llaves de acceso a archivadores o dependencias. – Si dispones de llaves de acceso a archivadores o dependencias donde se contengan soportes o documentos en papel con datos de carácter personal, debes custodiarlas debidamente.

Almacenamiento de soportes o documentos en papel. – Debes guardar todos los soportes o documentos que contengan información de carácter personal en un lugar seguro cuando éstos no estén siendo usados, particularmente, fuera de la jornada laboral. Los armarios, archivadores u otros elementos en los que se ubiquen los soportes de información deberán disponer de mecanismos de cierre que impidan el acceso a personas no autorizadas. Cuando estos soportes o documentos no se encuentren almacenados, por estar siendo revisados o tramitados, los debes custodiar e impedir, en todo momento, que un tercero no autorizado pueda tener acceso.

Fotocopiadoras, faxes o impresoras papeles con datos de carácter personal. – Cuando se imprima, fotocopie, digitalice o se remita por fax documentación, debe permanecer el menor tiempo posible en las bandejas de salida de los equipos implicados, para evitar que terceras personas puedan acceder a la misma. Conviene no olvidar retirar los originales de la fotocopiadora, impresora, escáner o fax una vez finalizado el proceso correspondiente. Si encuentras documentación abandonada en una fotocopiadora, impresora, escáner o fax, debes intentar localizar a su propietario para que éste la recoja inmediatamente. En caso de desconocer a su propietario o no localizarlo, ponlo inmediatamente en conocimiento de tu superior jerárquico.

Documentos no visibles en los escritorios, mostradores u otro mobiliario. – Debes mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en los escritorios, mostradores u otro mobiliario.

Desechado y destrucción de soportes o documentos en papel con datos personales. – No tires soportes o documentos en papel, donde se contengan datos personales, a papeleras abiertas, de modo que pueda ser legible o fácilmente recuperable por cualquiera. La destrucción de los documentos que contengan información no clasificada como pública, incluyendo las copias o reproducciones, se realizará mediante máquinas destructoras, de forma que se evite la recuperación o reconstrucción de la información con posterioridad.

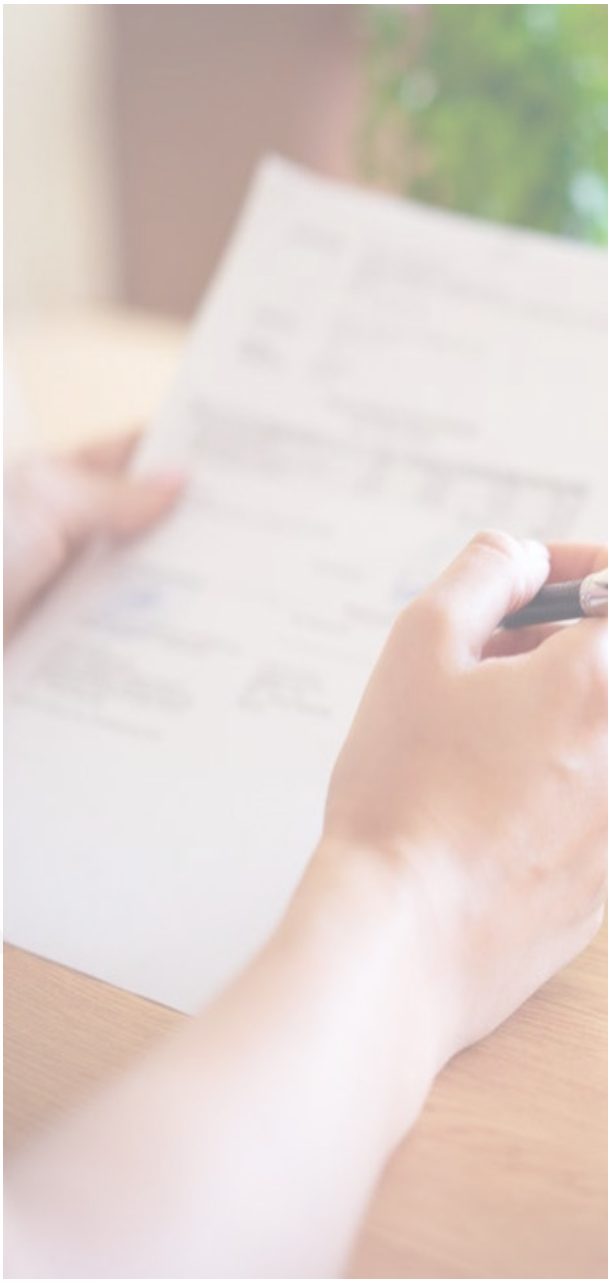
Traslado de soportes o documentos en papel con datos de carácter personal. – En los procesos de traslado de soportes o documentos, debes adoptar medidas dirigidas a impedir el acceso o manipulación por terceros, de manera que no pueda verse el contenido.

Envío de datos personales de categoría especial. - Si tienes que enviar a terceros ajenos a la Diputación documentos en papel que contienen datos de categoría especial (salud, ideología, religión, creencias, origen racial o étnico) lo debes hacer en sobre cerrado y, en cualquier caso, por medio de correo certificado o a través de una forma de correo ordinario que permita su completa confidencialidad.

"LA DESTRUCCIÓN DE LOS DOCUMENTOS SE REALIZARÁ MEDIANTE MÁQUINAS DESTRUCTORAS, DE FORMA QUE SE EVITE LA RECUPERACIÓN O RECONSTRUCCIÓN DE LA INFORMACIÓN CON POSTERIORIDAD".

¿PUEDEN SANCIONAR A LA DIPUTACIÓN DE VALENCIA POR NO TRATAR ADECUADAMENTE LOS DATOS PERSONALES EN SOPORTE PAPEL?

Una de las novedades que trajo consigo el 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 y por el que se deroga la Directiva 95/46/CE (RGPD) fue el endurecimiento del régimen sancionador, que incrementó notablemente la cuantía de las sanciones por el incumplimiento de lo previsto en la normativa de protección de datos. Por su parte, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) desarrolló el sistema de sanciones del RGPD, categorizando las infracciones en muy graves, graves y leves.



En el ámbito del sector público, el RGPD permite a los Estados establecer sus propias normas para regular su régimen sancionador. En el caso de España, la LOPDGDD contempla para determinadas categorías de responsables o encargados del sector público la sanción de **APERCIBIMIENTO**, acompañada de las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción. Entre estas categorías de responsables o encargados, se encuentra *"la Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local".* Asimismo, ha de tenerse en cuenta el **DAÑO REPUTACIONAL** que la sanción causaría a la organización.

"EL INADECUADO TRATAMIENTO DE LOS DATOS PERSONALES EN SOPORTE PAPEL POR PARTE DE LOS USUARIOS DE LOS SISTEMAS DE INFORMACIÓN DE LA DIPUTACIÓN PODRÍA CONLLEVAR UNA SANCIÓN DE APERCIBIMIENTO PARA LA ORGANIZACIÓN, ACOMPAÑADA DE LAS MEDIDAS QUE CONSIDERE LA AUTORIDAD DE CONTROL. ASIMISMO, HA DE TENERSE EN CUENTA EL DAÑO REPUTACIONAL QUE LA SANCIÓN CAUSARÍA A LA ORGANIZACIÓN".

SANCIONES DE LAS AUTORIDADES DE CONTROL RELACIONADAS CON EL TRATAMIENTO DE DATOS PERSONALES EN SOPORTE PAPEL

En la Resolución 754/2018, la Agencia Española de Protección de Datos (AEPD) sancionó a una Administración Pública por **depositar, en la vía pública, documentación relativa a reclamaciones efectuadas por ciudadanos de la localidad.**

En la Resolución 312/2010, la AEPD sancionó a una Administración Pública que, al realizar una reestructuración de las dependencias, **se deshizo de algunos documentos antiguos, que depositó, sin previa destrucción, en contenedores de la vía pública**. Se trataba de solicitudes de cursos, minutas de honorarios de profesores y registros de asistencia.

En el Procedimiento Sancionador 390/2019, la AEPD sancionó a una abogada por la **reutilización de papel con datos personales**, en concreto, por utilizar la reclamada, en dos ocasiones, para convocar a los inquilinos de un inmueble, un folio en cuyo reverso aparecían datos de terceros referidos a procedimientos en los que la reclamada había actuado como abogada.

En la Resolución 64/2011, la Autoridad Catalana de Protección de Datos (APDCAT) sancionó al Departamento de Enseñanza de la Generalitat de Catalunya por **depositar en la vía pública, junto al contenedor de papel y cartón, varios documentos** con la cabecera del Departamento de Enseñanza que contenían datos de carácter personal, entre otros, relativos a la salud de los interesados.

En la Resolución de la APDCAT 4/2014, se sancionó a una Administración Pública por **almacenar documentos en papel con datos personales sin cerradura.**

En el Procedimiento Sancionador de la APDCAT 18/2013, se sancionó a una Administración Pública por **depositar información con datos personales en un carro móvil** con varias bandejas sin cierre, ubicado en una planta de su sede, en un espacio completamente abierto, de modo que el conjunto de personas que prestaban servicio al conjunto de unidades de la organización, e incluso las visitas, podían acceder a la documentación mencionada.

En el Procedimiento Sancionador 32/2020 de la APDCAT, se sancionó a una Administración Pública por **remitir las comunicaciones y/o notificaciones a través de correo postal con sobres abiertos** y, por tanto, dejando el contenido de la carta accesible al cartero y a terceras personas.

En el Procedimiento Sancionador 10/2021, la APDCAT sancionó a una Administración Pública por **dejar, en la Sala de Plenos, varios documentos que contenían datos de carácter personal**, en concreto: la relación de los nombres y apellidos de dieciocho Policías Locales de nueva incorporación, junto sus fotografías y datos identificativos.

MATERIAL COMPLEMENTARIO

- Resolución R/00754/2018 (AEPD). Consulta este enlace.
- Resolución R/00312/2010 (AEPD). Consulta este enlace.
- Procedimiento PS/00390/2019 (AEPD). Consulta este enlace.
- Resolución 4/2014 (APDCAT). Consulta este enlace.
- Procedimiento Sancionador 18/2013 (APDCAT). Consulta este enlace.
- Resolución 64/2011 (APDCAT). Consulta este enlace.
- Procedimiento Sancionador 32/2020 (APDCAT). Consulta este enlace.
- Procedimiento sancionador 10/2021 (APDCAT). Consulta este enlace.
- Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal en la Diputación Provincial de Valencia, aprobado por acuerdo del Pleno de la Corporación de fecha 18 de junio de 2013 -BOP 159, de 6 de julio-.
- Decreto nº 6111, de 26 de junio de 2015, Normas de Seguridad para los Usuarios de los Sistemas de Información. Diputación Provincial de Valencia.

NOTICIAS

- **La APDCAT pone en marcha una campaña con consejos dirigidos a la ciudadanía para proteger su privacidad en las redes sociales.** La APDCAT ha puesto en marcha una campaña de difusión para promover un uso responsable de las redes sociales entre la ciudadanía, que incluye seis recomendaciones para no perder el control de los datos personales en estos canales, cada vez más utilizados. Sigue leyendo en este enlace.

- **Los ciberincidentes de tipo *ransomware* siguen siendo el origen de una parte muy importante de las brechas de datos personales notificadas a la AEPD.** Los ciberincidentes de tipo *ransomware* han vuelto a ser el origen de una parte muy importante de las brechas de datos personales notificadas a la AEPD durante el mes de julio, según el último informe de Notificaciones de Brechas de Datos Personales publicado por la AEPD. Casi la mitad de las notificaciones indican haber sufrido un incidente de este tipo. Consulta el informe en este enlace.

- **La AEPD se pronuncia sobre la viabilidad de que los particulares instalen "mirillas electrónicas" con videocámara en la puerta de su vivienda.** Entiende la Agencia que su mera instalación no supone, *a priori,* un mecanismo de control de las entradas/salidas de los vecinos, ni menos aún un hipotético "tratamiento de datos", ni es la finalidad para la que se concibe. En caso de "tratamiento", estará justificado cuando resulte necesario para proteger los derechos e intereses del propietario, generalmente su derecho a la integridad física y a la propiedad. Por tanto, el criterio de la AEPD es que si no existe una prueba objetiva que acredite un uso desproporcionado del dispositivo, el mismo es acorde a la finalidad concebida. Consulta la Resolución en este enlace.