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 30| Diciembre 2022

CORREO ELECTRÓNICO Y PROTECCIÓN DE DATOS PERSONALES

Í N D I C E

CORREO ELECTRÓNICO Y PROTECCIÓN DE DATOS PERSONALES

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

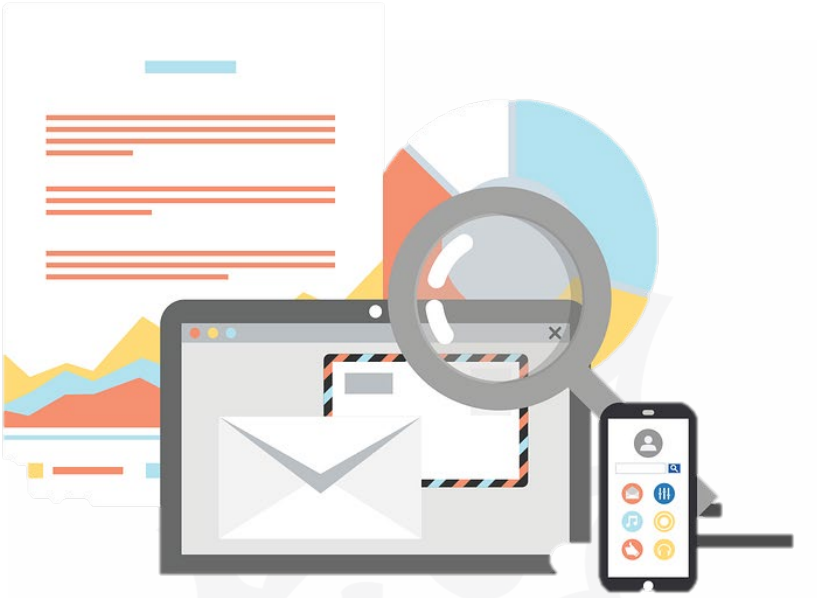
Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

LA DIRECCIÓN DE CORREO ELECTRÓNICO COMO DATO PERSONAL



El correo electrónico es un sistema de mensajería que permite la transmisión de mensajes entre usuarios sin necesidad que estén conectados al mismo tiempo. Las direcciones de correo electrónico de estos usuarios son el conjunto de palabras o signos que identifican al emisor o al receptor de un mensaje de correo electrónico y que se elaboran a partir de un conjunto de palabras o signos libremente escogidos, normalmente por su titular o por la organización a la cual pertenece, con el único límite de que esta dirección no coincida con la de otra persona. Están formadas por una identificación del usuario, seguido del signo @ y, a continuación, el dominio (identificación facilitada por el proveedor del servicio de correo, con un punto, y unas siglas que pueden identificar la actividad de la organización (por ej. ".org") o las siglas del país (por ej. ".es").

Pero **¿podemos considerar las direcciones de correo electrónico datos personales?** A estos efectos, las autoridades en materia de protección de datos distinguen:

DIRECCIONES PERSONALIZADAS

Son aquellas que incorporan información de su titular, como el nombre, apellidos, iniciales, cargo, número identificativo, etc. En estos casos, la dirección **identifica directamente a la persona titular de la cuenta**, por lo que **se trata de un dato personal.**

Ejemplos de direcciones personalizadas

- anaperez@dominio.es
- a.perez@dominio.es
- directora@dominio.es
- id3453@dominio.es

DIRECCIONES NO PERSONALIZADAS

Son aquellas que no parecen contener información sobre su titular, utilizando, por ejemplo, una combinación alfanumérica abstracta o sin ningún significado. En estos casos, **la dirección, por sí sola, no identifica a su titular, pero éste puede ser fácilmente identificable sin un esfuerzo desproporcionado**, bien porque la dirección puede aparecer junto con otros datos que permiten su identificación, bien por el contenido del mensaje, bien a través de los datos de que dispone el servidor de correo. Este tipo de direcciones **también deben considerarse dato personal**, ya que podrían permitir identificar de forma indirecta a su titular.

Ejemplos de direcciones no personalizadas

xyz80@dominio.es

DIRECCIONES GENÉRICAS

Cuando la dirección responde a una cuenta genérica, de uso compartido o de un área de la organización, esta no suele poder vincularse a una persona física, sino que puede ser atendida por usuarios diferentes y, **en principio, no puede considerarse un dato personal**. **Sin embargo, no se puede descartar, en función de la estructura de la organización (por ejemplo, en unidades unipersonales o supuestos en los que el acceso al correo esté limitado a una única persona), que se pueda vincular una dirección genérica con una persona identificada o identificable, en cuyo caso la dirección podría ser también un dato personal.**

Ejemplos de direcciones genéricas

consultas@dominio.es

administración@dominio.es

EN DEFINITIVA, LA DIRECCIÓN DE CORREO ELECTRÓNICO, CON LA EXCEPCIÓN MENCIONADA RELATIVA A LAS DIRECCIONES GENÉRICAS, PERMITE IDENTIFICAR DIRECTA O INDIRECTAMENTE A SU TITULAR, POR LO QUE ES UN DATO PERSONAL Y, EN CONSECUENCIA, SU TRATAMIENTO ESTÁ SOMETIDO A LAS REGLAS Y PRINCIPIOS DE LA NORMATIVA DE PROTECCIÓN DE DATOS.

EL CONTENIDO DEL CORREO ELECTRÓNICO TAMBIÉN REVELA INFORMACIÓN PERSONAL

En un correo electrónico figura diversa información que se puede considerar como dato de carácter personal, en la medida en que nos ofrezca información sobre una persona física identificable.

DIRECCIÓN DE CORREO DEL EMISOR Y DESTINATARIO O DESTINATARIOS

Como ya adelantábamos, la dirección de correo se puede vincular fácilmente a una persona física. En ocasiones, la misma dirección ya facilita su identificación. En otros casos, en el campo correspondiente a la dirección, junto con ella, o incluso sustituyéndola, aparece la identificación de la persona que es su titular.

ASUNTO

Conviene que el asunto describa de forma concisa la naturaleza o el contenido del mensaje y, si es posible, se evite incluir en él datos de carácter personal. El grado de confidencialidad de los datos que se incluyan en él será menor que el de la información que contiene el cuerpo del mensaje, dado que la simple visualización de la bandeja de entrada o salida permite leer el asunto.

CUERPO DEL MENSAJE

Es el contenido del mensaje. Puede consistir en un texto, con formato o sin, o en imágenes, que pueden contener datos de carácter personal. También puede contener datos personales o enlaces a páginas web o documentos que contengan datos personales.

PIE DE FIRMA

Es el texto que aparece debajo de la identificación de quién suscribe el mensaje. Normalmente, ofrece información sobre el cargo y la organización a la cual pertenece el emisor. A menudo, los sistemas de correo electrónico ofrecen la posibilidad de incorporar en los mensajes de correo un pie de firma de forma automática.

DOCUMENTOS ADJUNTOS

El correo electrónico permite adjuntar al mensaje imágenes, documentos, vídeos o audio. Para evitar revelaciones indebidas de información, conviene extremar la prudencia cuando se adjunten ficheros.

EN UN CORREO ELECTRÓNICO FIGURA DIVERSA INFORMACIÓN QUE SE PUEDE CONSIDERAR COMO DATO PERSONAL, EN LA MEDIDA EN QUE NOS OFREZCA INFORMACIÓN SOBRE UNA PERSONA FÍSICA IDENTIFICABLE: ASUNTO, CUERPO DEL MENSAJE, PIE DE FIRMA O DOCUMENTOS ADJUNTOS.

BUENAS PRÁCTICAS PARA PRESERVAR LA CONFIDENCIALIDAD EN LA REMISIÓN DE CORREOS ELECTRÓNICOS

Uso exclusivo para la remisión de correos relacionados con las funciones encomendadas. – El correo corporativo debe utilizarse, única y exclusivamente, para la realización de las funciones encomendadas al personal.

Copia oculta (CCO). – Utiliza la copia oculta cuando envíes correos a múltiples direcciones y estos no tengan por qué conocer la dirección de correo electrónico del resto de personas destinatarias.

Reenvío de correos. – Asegúrate de que los reenvíos de mensajes previamente recibidos se transmitan únicamente a los destinatarios apropiados.

Redes públicas. – Evita remitir correos electrónicos si estás conectado a redes públicas.

Remisión de datos sensibles. – Hay que velar por la seguridad de estos datos y, si procede, valorar el uso de medios técnicos, como técnicas de cifrado, para asegurar que el contenido no será interceptado por terceros.

Notificación de anomalías. – Notifica a este Departamento cualquier tipo de anomalía detectada en el uso del correo electrónico.

REALIZANDO UN USO CORRECTO DE NUESTRAS CUENTAS CORPORATIVAS DE CORREO ELECTRÓNICO PROTEGEREMOS NUESTRA ORGANIZACIÓN.

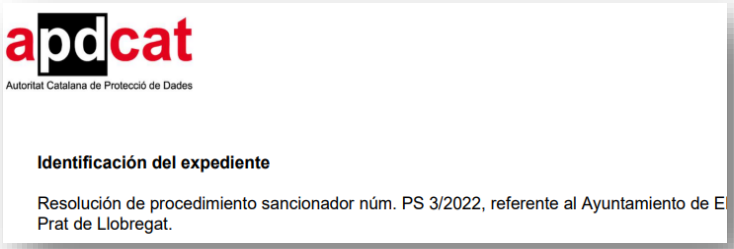
ÚLTIMAS RESOLUCIONES SANCIONADORAS RELACIONADAS CON LA REMISIÓN DE CORREOS ELECTRÓNICOS

La AEPD sanciona al Servicio de Salud de Castilla La Mancha por enviar un email a varios de sus trabajadores con sus nombres, categoría profesional, resultados de las pruebas de Covid-19, si habían padecido la enfermedad y si esto había conllevado una baja laboral.

El email no contenía únicamente la información relativa a cada destinatario sino también la de todos los demás. La AEPD consideró que las medidas de seguridad de la entidad reclamada no eran adecuadas en el momento de producirse el incidente objeto de reclamación, debiendo ser mejoradas porque no habían sido suficientes para evitar los hechos denunciados. Así las cosas, se consideró que la entidad reclamada había infringido los artículos 9, 5.1. f) y 32 del RGPD, al tratar datos de salud especialmente protegidos, por violar el principio de integridad y confidencialidad y, finalmente, por no adoptar las medidas de seguridad necesarias para garantizar la protección de los datos de carácter personal de su personal. Por todo ello, impone tres sanciones de **APERCIBIMIENTO**.

La AEPD sanciona a una entidad por enviar un correo electrónico a una pluralidad de clientes sin usar el método de Copia Oculta.

La entidad reclamada, mediante correo electrónico remitido a una pluralidad de clientes, expuso sin su consentimiento su dirección de correo electrónico a terceros. La AEPD consideró que la entidad reclamada, al remitir un correo electrónico de manera plural sin utilizar la modalidad de copia oculta, cedió sus datos a terceros sin causa que lo legitimara y, por tanto, había realizado un tratamiento de sus datos personales contrario a derecho. Así las cosas, la entidad reclamada habría infringido los artículos 5.1 f) y 32 del RGPD, al violar el principio de integridad y confidencialidad, así como no adoptar las medidas de seguridad necesarias para garantizar la protección de los datos de carácter personal de sus clientes, al no utilizar la modalidad de copia oculta en la remisión del correo electrónico. Por todo ello, impone una **MULTA** de 6.000€ (infracción del art. 5.1.f) RGPD) y 3.000€ (infracción del art. 32 RGPD).

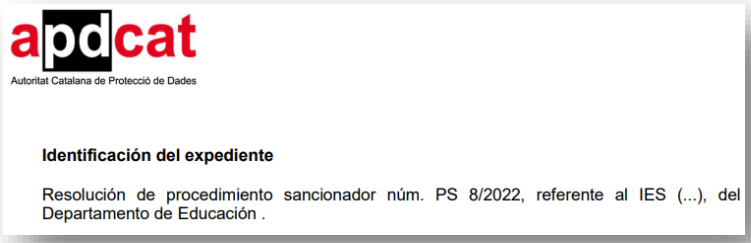

apdcat
Autoritat Catalana de Protecció de Dades

Identificación del expediente

Resolución de procedimiento sancionador núm. PS 3/2022, referente al Ayuntamiento de El Prat de Llobregat.

La APDCAT sanciona al Ayuntamiento de El Prat de Llobregat por el envío de un correo electrónico sin copia oculta, revelando información dirigida a título particular.

Se **APERCIBE** al Ayuntamiento como responsable de una infracción por vulneración del principio de confidencialidad (art. 5.1.f) RGPD), por el hecho de haber enviado un correo sin copia oculta a los trabajadores del cuerpo de la Policía Local, identificándolos con nombre y apellidos y dirección electrónica, revelando la identidad de aquellos que todavía no habían realizado la sesión formativa de prevención por la covid-19, y que consiguientemente figuraban en una bolsa de personas "morosas".

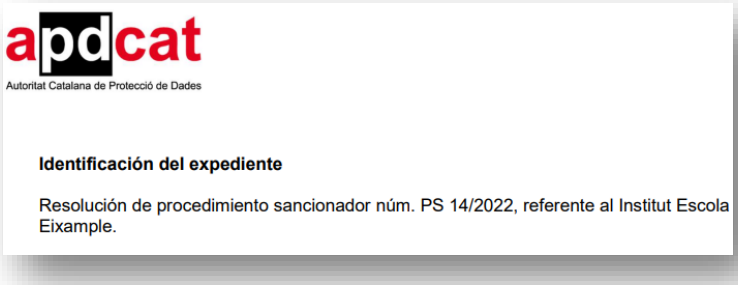

apdcat
Autoritat Catalana de Protecció de Dades

Identificación del expediente

Resolución de procedimiento sancionador núm. PS 8/2022, referente al IES (...), del Departamento de Educación .

La APDCAT sanciona un instituto por la remisión de comunicaciones a un correo electrónico erróneo.

Durante todo un curso escolar el IES envió las comunicaciones y notas de un alumno a un correo electrónico que no era lo de los padres del alumno, sino a una tercera familia del IES, hecho que comportó la vulneración del principio de confidencialidad (art. 5.1.f) RGPD). Por este motivo, se impone una sanción de **APERCIBIMIENTO.**


apdcat
Autoritat Catalana de Protecció de Dades

Identificación del expediente

Resolución de procedimiento sancionador núm. PS 14/2022, referente al Institut Escola Eixample.

La APDCAT sanciona a un instituto por la remisión de comunicaciones a un correo electrónico erróneo.

La APDCAT resuelve **APERCIBIR** al Instituto Escuela Eixample del Departamento de Educación dado que se acredita que desde la Escuela se habría hecho llegar a los padres y madres de los alumnos (115 personas) un correo, sin emplear la opción de la copia oculta, lo que propició que todos los destinatarios pudieran acceder a la dirección de correo del resto de personas a quienes se dirigía el mensaje. El contenido del correo informaba sobre el proceso de vacunación contra la Covid-19 en el centro.

MATERIAL COMPLEMENTARIO

- Recomendación 1/2013 sobre el uso del correo electrónico en el ámbito laboral. (APDCAT). Consulta la Recomendación en este enlace.
- Informe 0437/2019, sobre si el correo electrónico ha de considerarse dato personal (AEPD). Consulta el informe en este enlace.
- Expediente N.º: EXP202200447 (AEPD). Consulta la resolución en este enlace.
- Expediente N.º: PS/00293/2022 (AEPD). Consulta la Resolución en este enlace.
- PS 3/2022 (APDCAT). Consulta la Resolución en este enlace.
- PS 8/2022 (APDCAT). Consulta la Resolución en este enlace.
- PS 14/2022 (APDCAT). Consulta la Resolución en este enlace.
- ¿Seguridad en el correo electrónico? Sí, en tan solo 10 pasos (INCIBE). Consulta este enlace.
- Correo electrónico. Informe de buenas prácticas (CCN). Consulta este enlace.
- Privacidad y Seguridad en Internet. Ficha 14: Quiero proteger mi correo electrónico (AEPD, INCIBE, OSI). Consulta este enlace.
- Uso del correo electrónico (INCIBE). Consulta este enlace.

NOTICIAS

- **La AEPD publica una Guía y Herramienta básica de anonimización.** La Agencia ha traducido la Guía básica de Anonimización de la Autoridad de Protección de Datos de Singapur por su valor didáctico y especial interés para responsables, encargados de tratamientos y delegados de protección de datos. La guía se complementa con una herramienta gratuita de anonimización de datos, que la AEPD pone a disposición de las organizaciones. Consulta la información en este enlace.

- **La APDCAT sanciona a una Entidad Local por no tener actualizados los datos de contacto del Delegado de Protección de Datos en su web.** La persona que formuló denuncia contra el Ayuntamiento expuso que, con intención de ponerse en contacto con el Delegado de Protección de Datos (DPD) del Ayuntamiento, observó que en la página web de la corporación constaba un delegado y datos de contacto que no coincidían con lo que constaba inscrito en el registro de la APDCAT y que esto provocó que no supiera a quién debía dirigirse. Consulta la Resolución en este enlace.

- **La APDCAT emite un informe en relación con una solicitud de acceso a información de una concejala relativa a los fichajes del personal.** En este caso, concluye que otorgar el acceso por parte de la concejalía a la información solicitada, previamente seudonimizada, podría permitir controlar igualmente la actuación del Ayuntamiento respecto de su función de vigilancia y control del cumplimiento del régimen horario establecido, de forma que pueda identificar, sin necesidad de sacrificar la privacidad de las personas afectadas, patrones de incumplimiento horario en determinados miembros de la plantilla (respecto de los cuales podría estar justificado a posteriori conocer su identidad) y poder exigir al consistorio la adopción de medidas de control efectivas o, en su caso, responsabilidades. Consulta el informe en este enlace.