Diputació de València | Protecció de Dades i Seguretat de la Informació

CIRCULAR INFORMATIVA 2/24 DEL DEPARTAMENTO DE PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN SOBRE GARANTÍAS DE PRIVACIDAD EN EL SISTEMA INTERNO DE INFORMACION Y DEFENSA DE LA PERSONA INFORMANTE (CANAL DE DENUNCIAS)

La Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción –en adelante, LPI- establece la obligación de las personas jurídicas afectadas por sus disposiciones de disponer de un Sistema interno de información que garantice, en el seno de la organización obligada, la existencia de un cauce preferente para la comunicación de las infracciones normativas comprendidas en el artículo 2 de la LPI y la protección a las personas informantes frente a posibles represalias. La Diputación de Valencia, en tanto entidad que integra el sector público –artículo 13.1.a)- se encuentra sometida a dicha obligación. Gracias a este canal se posibilita que cualquier persona, incluido el personal funcionario público, pueda comunicar infracciones o conductas corruptas o fraudulentas de las que tenga conocimiento en relación con la Diputación de Valencia.

En este sentido, la LPI establece una serie de garantías de privacidad para las personas informantes que deben ser implementadas por la Diputación de Valencia:

1.- Garantizar el anonimato de la persona informante

La LPI permite la presentación de comunicaciones -esto es, denuncias- anónimas. Anonimidad no es lo mismo que anonimización. Los datos personales anonimizados son aquellos que han sido tratados precisamente para desvincularlos totalmente de la persona física a la que hacen referencia, de forma que este proceso resulte irreversible, es decir, que ya no puedan posteriormente volver a ser asociados a una persona física. Pero, por su propia naturaleza, el proceso de anonimización conlleva un tratamiento de datos personales. Por el contrario, la anonimidad hace referencia a los datos ya anónimos, de forma que quien los trata por primera vez ya se encuentra con la imposibilidad de asociarlos a una persona física identificada o identificable. Este es el supuesto recogido por la LPI, en el que el responsable del sistema interno de información no trataría en ningún caso datos personales de la persona informante que optase por este tipo de denuncia.

Esta es una copia impresa del documento electrónico generada por la aplicación informática Portafirmas.
Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://www.sede.dival.es/opencms/opencms/portal/index.jsp?opcion=verifica

Es por esto que el Sistema debe garantizar este anonimato al momento de la presentación de la comunicación y, en consecuencia, no debe recoger NINGÚN dato que permita la identificación, directa o indirecta, de la persona física informante; bien a través de identificadores directos (nombres, apellidos, cargo, DNI, etc.) o indirectos (IP, hora de conexión, ID del dispositivo, MAC, cookies, fingerprinting, etc.). Esto resulta especialmente relevante cuando la persona informante es empleada o miembro de la propia organización y realiza la comunicación utilizando dispositivos y entornos tecnológicos internos.

La simple omisión de los datos identificativos de la persona física informante no implica que se trate de comunicación anónima, **puesto que la persona ha sido o puede llegar a ser identificada examinando otra información asociada**. Realmente, se estaría operando un procedimiento de anonimización o disociación de los datos y no se trataría, en puridad, de una comunicación o denuncia por persona anónima.

Téngase en cuenta que la voz también es considerada un dato de carácter personal, en la medida que permite la identificación de una persona física. De modo que el Sistema de información que recoja, por ejemplo, llamadas de personas físicas, que no se identifican con nombre y apellidos, en rigor, no supone una comunicación anónima, ya que también podría llegar a ser identificada.

Es aconsejable para las personas informantes que deseen acogerse al anonimato el uso de herramientas tecnológicas caracterizadas por sus altas garantías de anonimidad, como navegadores del estilo TOR y otras utilidades asociadas a la red TOR (The Onion Router), como OnionShare o Onion Mail**.**

Se aconseja a los/as empleados/as la realización del curso de formación "*Normativa, procedimientos y herramientas internas para el cumplimiento de la legislación de protección de datos y seguridad de la información en la Diputación de Valencia*", del Plan General de Formación 2024, **entre cuyos contenidos se mostrará cómo instalar y utilizar estas herramientas.**

2.- Garantizar la confidencialidad de la identidad de la persona informante

La confidencial es uno de los principios fundamentales del Sistema interno de información. En el supuesto de que la persona informante no haya optado por la denuncia anónima, su identidad solo podrá ser comunicada a la autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora (artículo 33.3 LPI). La confidencialidad se hace extensiva a la identificación de denunciados y otros afectados, así como de la información asociada a todos ellos. La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública.

Esta es una copia impresa del documento electrónico generada por la aplicación informática Portafirmas.
Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://www.sede.dival.es/opencms/opencms/portal/index.jsp?opcion=verifica

La confidencialidad también se manifiesta a la hora de acceder y tratar la información. El artículo 32 LPI establece que el acceso a los datos personales contenidos en el Sistema interno de información quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:

a) El Responsable del Sistema y a quien lo gestione directamente.

b) El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo.

c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

d) Los encargados del tratamiento que eventualmente se designen.

e) El delegado de protección de datos.

Intervención del Delegado de protección de datos en el Sistema interno de información

Cualquier persona cuyos datos personales sean objeto de tratamiento en el Sistema interno de información, que considere que en seno del Sistema se han conculcado los principios y derechos recogidos en la normativa sobre protección de datos, puede ponerlo en conocimiento del Delegado de protección de datos. El artículo 38.4 RGPD indica que "*Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento*".

Singularmente, el personal empleado público puede poner en conocimiento del Delegado situaciones de violación de derechos de protección de datos en el seno del Sistema interno de información, tales como el acceso, la revelación o comunicación de datos a personas no legitimadas para ello; el incumplimiento del deber de secreto y confidencialidad o la inobservancia de las medidas de seguridad de la información. El Delegado intervendrá incluso si quien informa de estas situaciones no es la persona afectada.

El Delegado, tras la valoración de la información aportada, procederá, si considera la existencia de fundamento suficiente, a investigar los hechos y concluir con las acciones pertinentes en función del resultado de las evidencias y, en su caso, de la gravedad de la conculcación.

Esta es una copia impresa del documento electrónico generada por la aplicación informática Portafirmas.
Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://www.sede.dival.es/opencms/opencms/portal/index.jsp?opcion=verifica

Debe recordarse que el Delegado de protección de datos es una figura independiente, que no puede recibir instrucciones en lo que respecta al desempeño de sus funciones (art. 38.3 RGPD) y que está obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones (art. 38.5 RGPD).

Se puede contactar con el Delegado de protección de datos en **pdp@dival.es**

Valencia, 27 de Febrero de 2024

Eusebio Moya López

DELEGADO DE PROTECCIÓN DE DATOS

DE LA DIPUTACIÓN DE VALENCIA

Esta es una copia impresa del documento electrónico generada por la aplicación informática Portafirmas.
Mediante el código de verificación puede comprobar la validez de la firma electrónica de los documentos firmados en la dirección web: https://www.sede.dival.es/opencms/opencms/portal/index.jsp?opcion=verifica