SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

PRO.PD-07

PROCEDIMIENTO

DE NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD DE LOS DATOS PERSONALES.

Diputación de Córdoba

DIPUTACIÓN DE CÓRDOBA

CONTROL DE DOCUMENTACIÓN:

CÓDIGO:	PRO.PD-07	DOCUMENTO:	PROCEDIMIENTO DE NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD DE LOS DATOS PERSONALES

REVISIÓN NÚMERO:	00	FECHA DE ENTRADA EN VIGOR:	15/11/2019

ES ORIGINAL:	☒	ES COPIA CONTROLADA:	☐	ES COPIA NO CONTROLADA:	☐

ELABORADOR POR:	REVISADO POR:	APROBADO POR:
TIC4YOU SL	DAVID YUBERO REY DPD DIPUTACIÓN DE CÓRDOBA	COMITÉ DE SEGURIDAD DE LA INFORMACIÓN
		FECHA:
		15/11/2019

CONTROL DE CAMBIOS:

REVISIÓN Nº:	FECHA:	APARTADO MODIFICADO:	CAUSA DEL CAMBIO:	ENTRADA EN VIGOR:

DOCUMENTACIÓN OBSOLETA:	☐	FECHA:	

CLASIFICACIÓN DE LA INFORMACIÓN:

PÚBLICA:	☐	PUBLICABLE:	☒	USO INTERNO:	☐	CONFIDENCIAL:	☐	SECRETA:	☐

Í N D I C E

1. OBJETO

El objeto de este procedimiento es establecer la operativa para la notificación de violaciones de seguridad que hayan sufrido nuestro ayuntamiento en lo que a datos de carácter personal se refiere.

2. ALCANCE

Este procedimiento es de aplicación a todos los responsables o encargados de tratamiento que, de conformidad con el artículo 33 del REGLAMENTO (UE) 2016/679 del Parlamento Europeo y del consejo de 27 de abril de 2016 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 (Reglamento general de protección de datos-RGPD), tienen la obligatoriedad de notificar todas las violaciones de seguridad que haya sufrido su ayuntamiento a la autoridad de control.

3. REFERENCIAS

Para la elaboración de este procedimiento se ha utilizado como referencia:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 (Reglamento general de protección de datos). *Artículos 33 y 34, considerandos 85, 86, 87 y 88*.
- Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 (Reglamento general de protección de datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Directiva (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva NIS) - Artículos 14, 16 y 20.
- REGLAMENTO (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (eIDAS) - Artículos 10, 17.6 y 19.3 y Considerandos 38 y 39.
- Directiva (UE) 2008/114 DEL CONSEJO, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (vigente en aquellos artículos que no contradigan el RGPD).
- Real Decreto1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 (vigente en aquellos artículos que no contradigan el RGPD).
- Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

- Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Artículos 24,36 y Disposición Adicional Cuarta.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de Protección de las Infraestructuras Críticas.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Ley General 9/2014, de 9 de mayo, de Telecomunicaciones - Artículos 41 y 44.
- REGLAMENTO (UE) 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de brecha de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, que regula la Gestión de incidentes de ciberseguridad que afecten a la red de Internet. Disposición adicional novena.
- Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento publicada por la AEPD.
- Guía para la gestión y notificación de brechas de seguridad publicada por la AEPD.
- Directrices sobre notificación de brechas de la seguridad de los datos personales, adoptadas el 3 de octubre de 2017 por el Grupo de Trabajo del Artículo 29 (WP29).
- Directrices sobre notificación de incidentes graves de conformidad con la Directiva (EU) 2015/2366 (PSD2), adoptadas el 27 de julio de 2017 por la Autoridad Bancaria Europea.
- UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.
- ISO/IEC 29100:2011 Information technologi – Security Techniques – Privacy framework

4. RESPONSABILIDADES

Será responsabilidad de la Diputación de Córdoba junto con el Instituto Provincial de Bienestar Social, el Instituto Provincial de Cooperación con la Hacienda Local, el Instituto Provincial de Desarrollo Económico, el Consorcio Provincial de Prevención y Extinción de Incendios, el Patronato Provincial de Turismo de Córdoba, la Agencia Provincial de la Energía, la Fundación Provincial de Artes Plásticas Rafael Botí, la Empresa Provincial de Aguas de Córdoba, la Empresa Provincial de Residuos y Medio Ambiente y la Empresa Provincial de Informática (en adelante, la Diputación de Córdoba y su sector público institucional) *(Responsable o Encargado de Tratamiento)* el notificar a la autoridad de control pertinente, en este caso la AEPD, cualquier violación de seguridad que se haya producido en el ayuntamiento y que afecte a los datos de carácter personal de éste.

5. DESARROLLO

5.1. NOTIFICACIÓN DE UNA VIOLACIÓN DE LA SEGURIDAD A LA AUTORIDAD DE CONTROL

Este apartado se aplica a las violaciones de datos personales que afectan a los datos personales con respecto a los cuales el ayuntamiento actúa como responsable del tratamiento.

En caso de producirse alguna violación de seguridad en los sistemas definidos y adoptados por la Diputación de Córdoba o por su sector público institucional, y que afecte a datos de carácter personal, será responsabilidad del ayuntamiento notificar de manera inminente, o en su defecto en un máximo de 72 horas, a la autoridad de control, que en este caso recae en la Agencia Española de Protección de Datos. Si no pudiere notificarse en el plazo previsto, dicha notificación deberá acompañar las indicaciones pertinentes que motiven la dilación en el plazo de comunicación.

Las notificaciones de violación de datos personales a la autoridad de control deben ser realizadas por la persona designada en el ayuntamiento utilizando el formulario establecido a través de la sede electrónica de la AEPD: https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf. La persona designada en el ayuntamiento deberá llevar un registro de todas las notificaciones, y de todas las demás comunicaciones con la autoridad de control relacionadas con el incumplimiento, como parte del RG.PD-02_PRO.PD-07 Registro de seguimiento de incidencias.

Si la violación de seguridad no constituye un riesgo para los derechos y las libertades de las personas físicas, no será necesario dicha comunicación a la AEPD. La persona designada en el ayuntamiento deberá dejar constancia de cualquier decisión de no notificar a la autoridad de control. Este registro debe incluir las razones de la persona designada para creer que es improbable que la violación suponga un riesgo para los derechos y libertades de la persona física. Este registro se almacenará como parte del RG.PD-01_PRO.PD-07 Registro de Brechas / Incidencias.

En la medida en que el ayuntamiento no pueda proporcionar a la autoridad supervisora toda la información especificada en el anexo 1 en el momento de la notificación inicial a la autoridad de control, el ayuntamiento debe hacer todos los esfuerzos razonables para determinar la información que falta. Esta información deberá ser facilitada a la autoridad de control por la persona designada en el ayuntamiento, a medida que esté disponible. La persona designada debe crear un registro de las razones de cualquier notificación retrasada. Este registro se almacenará como parte del registro de incumplimiento de datos personales del ayuntamiento.

El ayuntamiento debe mantener informada a la autoridad de control de los cambios en los hechos comprobados por el ayuntamiento que afecten cualquier notificación hecha.

Si la violación entrañara un alto riesgo para los derechos y libertadas de las personas físicas afectadas, se comunicará a las personas interesadas sin dilación según lo descrito en el apartado 5.2 del presente procedimiento, sin perjuicio de la que se realizara a la autoridad de control.

5.2. COMUNICACIÓN DE VIOLACIONES DE SEGURIDAD AL INTERESADO.

Conforme al artículo 34 del RGPD, será necesario la comunicación de la violación de la seguridad de los datos personales al interesado cuando ésta constituya un riesgo alto para sus derechos y libertades.

Dicha comunicación se realizará en un lenguaje claro y conciso, describiendo como mínimo la naturaleza de la violación de la seguridad así como los puntos 2, 3 y 4 del apartado 5.4.

Las notificaciones de violación de datos personales a los interesados afectados deberán contener al menos los puntos detallados en el Anexo 1 Notificación de la violación de datos personales al interesado. La notificación deberá enviarse a los interesados afectados por [medios adecuados]. La persona designada en el ayuntamiento deberá llevar un registro de todas las notificaciones, y todas las demás comunicaciones con los afectados relacionadas con el incumplimiento, como parte del RG.PD-02_PRO.PD-07 Registro de seguimiento de incidencias.

El ayuntamiento no tiene obligación de notificar al interesado afectado de una violación de datos personales si:

a) El ayuntamiento ha aplicado las medidas técnicas y organizativas de protección adecuadas (en particular las que hacen ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado), y dichas medidas se han aplicado a los datos personales afectados por la violación de los datos personales;
b) El ayuntamiento ha adoptado medidas posteriores que garanticen que ya no es probable que se materialice un alto riesgo para los derechos y libertades de los interesados;
c) Si la notificación al interesado supusiera un esfuerzo desproporcionado (en cuyo caso, en su lugar, habrá una comunicación pública o medida similar por la que se informe a los interesados de manera igualmente eficaz), disponiendo que la persona designada será responsable de determinar si se aplica este apartado, y que la persona designada deberá dejar constancia de cualquier decisión de no notificar a los interesados afectados. Este registro debe incluir las razones de la persona designada para creer que la violación no necesita ser notificada a los afectados. Este registro se almacenará como parte del RG.PD-01_PRO.PD-07 Registro de Brechas / Incidencias.

Si el ayuntamiento no está obligado a notificar a los interesados afectados una violación de los datos personales, el ayuntamiento podrá, no obstante, hacerlo cuando dicha notificación redunde en interés del ayuntamiento y/o de los interesados afectados.

5.3. NOTIFICACIÓN AL RESPONSABLE DEL TRATAMIENTO

Este apartado se aplica a las violaciones de datos personales que afectan a los datos personales con respecto a los cuales el ayuntamiento actúa como procesador de datos (encargado).

El ayuntamiento deberá notificar a los responsables del tratamiento afectados cualquier violación de los datos personales inmediatamente después de que haya sido constatada. Además, el ayuntamiento deberá cumplir con lo dispuesto en el contrato con el responsable del tratamiento de datos afectado en relación con dichas notificaciones.

Las notificaciones de violación de datos de carácter personal al responsable o responsables del tratamiento afectados deberán contener al menos los puntos detallados en el Anexo 2 Notificación de la violación de datos personales al responsable del tratamiento. La notificación deberá enviarse a los responsables del tratamiento afectados por, medios seguros y confidenciales. La persona designada en el ayuntamiento deberá llevar un registro de todas las notificaciones, y de todas las demás comunicaciones con el responsable o responsables afectados en relación con el incumplimiento, como parte del RG.PD-02_PRO.PD-07 Registro de seguimiento de incidencias.

En la medida en que el ayuntamiento no pueda facilitar a los responsables del tratamiento afectados toda la información especificada en el anexo 2 en el momento de la notificación inicial a los responsables del tratamiento afectados, el ayuntamiento deberá hacer todos los esfuerzos razonables para averiguar la información que falta. Esta información deberá ser facilitada por la persona designada al responsable o responsables del tratamiento afectados, a medida que esté disponible.

5.4. CONTENIDO DE LA NOTIFICACIÓN.

En resumen, el contenido de la notificación de la violación de seguridad a la que hace referencia todo el apartado 5 del presente procedimiento, y en virtud del artículo 33.3 del RGPD, deberá contener, al menos, la siguiente información:

1. Descripción de la naturaleza de la violación de seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número de aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
2. Comunicación del nombre y los datos de contacto del DPD o de otro punto de contacto en que se pudiera obtener más información sobre la violación de seguridad sufrida.
3. Descripción de las posibles consecuencias que pudieran tener la violación de la seguridad de los datos personales.
4. Descripción de las medidas adoptadas o propuestas por la Diputación de Córdoba o por su sector público institucional para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar a la AEPD toda esta información de manera simultánea, se realizará de manera paulatina y sin dilación conforme vaya estando disponible.

5.5. OTRAS NOTIFICACIONES

Sin perjuicio de las obligaciones de notificación establecidas en otras partes de este procedimiento, la persona designada también deberá considerar la posibilidad de notificar a terceros la violación de datos personales. Las notificaciones pueden ser requeridas por ley o por contrato.

6. REGISTROS/ANEXOS

- RG.PD-01_PRO.PD-07 Registro de Brechas / Incidencias.
- RG.PD-02_PRO.PD-07 Registro de seguimiento de incidencias.

- Documento de Notificación de Violaciones de la Seguridad a la AEPD (externo).
- Anexo 1 Notificación de la violación de datos personales al interesado.
- Anexo 2 Notificación de la violación de datos personales al responsable de tratamiento.

ANEXO 1 (NOTIFICACIÓN DE VIOLACIÓN DE DATOS PERSONALES AL INTERESADO)

Introducción

Esta notificación de violación de datos personales es realizada por el Delegado de Protección de Datos o por la Diputación de Córdoba o su sector público institucional.

Descripción de la violación de datos personales

Describa las circunstancias de la violación de los datos personales, incluyendo la fecha y hora en que el responsable del tratamiento tuvo conocimiento de la violación].

Categorías de datos personales afectadas

Especifíquense las categorías de datos personales de que se trate].

Consecuencias probables del incumplimiento

[Identificar las posibles consecuencias de la violación]

Medidas adoptadas para hacer frente al incumplimiento

[Describa las medidas adoptadas para hacer frente a la violación]

Medidas para mitigar el incumplimiento

Insertar detalles de las medidas que el interesado puede tomar para mitigar la violación de los datos personales].

Datos de contacto

El nombre de la persona responsable de la gestión de la infracción es[insértese el nombre], y[sus] O[sus] datos de contacto son los siguientes: [insertar datos de contacto].

ANEXO 2 (NOTIFICACIÓN DE VIOLACIÓN DE DATOS PERSONALES AL RESPONSABLE DEL TRATAMIENTO)

Introducción

Esta notificación de violación de datos personales es realizada por el Delegado de Protección de Datos o por la Diputación de Córdoba o su sector público institucional.

Descripción de la violación de datos personales

Describa las circunstancias de la violación de los datos personales, incluyendo la fecha y hora en que el responsable del tratamiento tuvo conocimiento de la violación].

Categorías de interesados afectados

Especifique las categorías de interesados afectados]

Número de interesados afectados

Insértese el número o número aproximado de personas afectadas].

Categorías de datos personales afectadas

Especifíquense las categorías de datos personales de que se trate].

Número de registros afectados

Insértese el número o número aproximado de registros de que se trate].

Consecuencias probables del incumplimiento

[Identificar las posibles consecuencias de la violación]

Medidas adoptadas para hacer frente al incumplimiento

[Describa las medidas adoptadas para hacer frente a la violación]

Datos de contacto

El nombre de la persona responsable de la gestión de la infracción es[insértese el nombre], y[sus] O[sus] datos de contacto son los siguientes: [insertar datos de contacto].