RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR POR INFRACCIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

Resolución	RPS-2024/043
Procedimiento Sancionador	PS-2023/038
Expediente	RCO-2022/090
Entidad incoada	Ayuntamiento de Vélez Rubio
Motivo de la reclamación	Se difunden datos personales de un conjunto de personas a través de la verificación telemática de la firma del documento de notificación de multas de tráfico, a través de un código QR
Artículos afectados	5.1.f y 32 RGPD

Abreviaturas:
RGPD. 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)
LOPDGDD. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
LOPDP. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
LTPA. Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía
ESTATUTOS CTPDA. Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, aprobados por Decreto 434/2015, de 29 de septiembre.
LPAC. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
LRJSP. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
ENS. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

ANTECEDENTES

Primero. Presentación de la reclamación.

Con fecha 23 de junio de 2022, tuvo entrada en el Consejo de Transparencia y Protección de Datos de Andalucía (en adelante, el Consejo) reclamación contra el Ayuntamiento de Vélez Rubio, por una presunta infracción de la normativa de protección de datos personales.

La reclamación se presentó originariamente ante la Agencia Española de Protección de Datos con fecha 6 de junio de 2022, dando esta traslado de la misma al Consejo por ser la autoridad de control competente en su tramitación.

En la citada reclamación se exponía:

> "Tras recibir una notificación de una multa, compruebo que incluye un código QR. Después de escanearlo se descargó un archivo en el que junto a la notificación de mi denuncia van otras notificaciones de otras personas a las que puedo tener acceso. Si alguna de estas personas hace lo mismo que yo también tendrá acceso al mismo archivo.
>
> Después pensé en comprobar si en otra denuncia que tengo de *[dd/mm/aa]* ocurría lo mismo, y sí, también se descargó otro archivo en el que junto a la notificación de mi denuncia iban otras notificaciones de otras personas.
>
> Con estos archivos, el Ayuntamiento de Vélez Rubio me ha dado acceso libremente a datos que supongo deben tener protegidos.
>
> También he podido comprobar que en las denuncias de un archivo ocurre algo anormal, como que el agente *[nnn]* y *[...]*".

Adjunto a la reclamación se aportaba copia de todas las notificaciones recibidas a nombre de terceras personas.

Segundo. Admisión a trámite de la reclamación y apertura de Actuaciones Previas de Investigación (arts. 65.5 y 67.1 LOPDGDD; Art. 55.2 LPAC).

La reclamación inició su tramitación con arreglo al procedimiento establecido en el Título VIII de LOPDGDD, y en virtud del artículo 67.1 de la misma, con fecha 13 de septiembre de 2022 el director del Consejo ordenó el inicio de actuaciones previas de investigación a los efectos de lograr una mejor determinación de los hechos y circunstancias que justificaran la tramitación de un posible procedimiento sancionador.

Tercero. Sobre las Actuaciones Previas de Investigación.

Con el objeto de completar la información relacionada con los hechos denunciados, el 13 de septiembre de 2022, desde el Consejo se requirió al Delegado de Protección de Datos (en adelante, DPD), o en su defecto, al responsable del tratamiento, para que remitiera información y documentación sobre las causas que habían motivado la incidencia y las actuaciones llevadas a cabo en relación con la reclamación. En concreto, se debía remitir:

- Motivos por los cuales no se procedió a la inhabilitación de la visualización y descarga del documento erróneamente difundido.
- Evidencias, si se ha producido, de la retirada posterior del mencionado documento.
- Motivos por los que se produjo la brecha de seguridad origen de los hechos reclamados.
- Indicación de las directrices y protocolos en relación con la firma de documentos que pudieran existir en el momento de la difusión incorrecta.

- Medidas que se han tomado con posterioridad para evitar la repetición de circunstancias similares en el futuro.

- Determinación de la actividad de tratamiento afectada por la incidencia objeto de la reclamación.

En respuesta al citado requerimiento, el 20 de octubre de 2022, tuvo entrada en el Consejo informe del DPD de la entidad incoada, del que se destaca, a los efectos de esta reclamación lo siguiente:

> "[...] El Ayuntamiento de Vélez Rubio remite escritos del Consejo de Transparencia y Protección de Datos de Andalucía al Comité de Seguridad de la Diputación, DPD de ese Ayuntamiento, en relación a:
>
> - Archivo de actuaciones sobre brecha de seguridad. Exp de ref: VS-2022/009. Fecha de registro de entrada en esta Diputación 16 de septiembre de 2022.
>
> - Admisión a trámite de la reclamación presentada contra el Ayuntamiento por presunta vulneración de la normativa de datos personales. Exp. de ref: RCO-2022.090. Fecha de entrada en esta Diputación 20 de septiembre de 2022.
>
> Con fecha de registro de entrada 3 de octubre de 2022, el Ayuntamiento de Vélez Rubio solicita a la Diputación de Almería la inhabilitación de la visualización del documento objeto de la reclamación.
>
> En atención al requerimiento recibido de ese Consejo, el Comité de Seguridad de la Información emite el siguiente informe en respuesta a las cuestiones que en este se plantean:
>
> 1. MOTIVOS POR LOS CUALES NO SE PROCEDIÓ A LA INHABILITACIÓN DE VISUALIZACIÓN Y DESCARGA DEL DOCUMENTO ERRÓNEAMENTE DIFUNDIDO.
>
> El 23 de mayo de 2022, la Diputación de Almería, como DPD del Ayuntamiento de Vélez Rubio y como ente gestor de los sistemas de la Red Provincial en los que está custodiada la información del Ayuntamiento de Vélez Rubio, así como el que ofrece herramientas para los servicios de tele administración, recibió información de una presunta vulnerabilidad sobre la normativa de protección de los datos personales por parte del Ayuntamiento.
>
> Se observa que el usuario del Ayuntamiento de Vélez Rubio había generado un documento para firmar con información de sanciones de diversos ciudadanos.
>
> Se trataba de un documento firmado.
>
> Dicho documento firmado no era posible su eliminación pues se perderían las propiedades de integridad y no repudio que caracterizan un documento firmado.
>
> La herramienta que usó el Ayuntamiento para realizar la firma se encuentra en los servidores del centro de proceso de datos de la Diputación de Almería y es la herramienta única de firma, tanto para la Diputación como para todas las entidades locales de Almería a las que se presta servicio.
>
> Se ha estado estudiando un sistema de bloqueo de documentos firmados.

Al tratarse de una herramienta global para toda la provincia, el sistema de bloqueo que se parametrizara en la aplicación afectaría a todos los documentos.

Tomar una decisión sobre el funcionamiento de una herramienta que afecta a tan elevado número de usuarios no era operativa. Por ello, se han estado estudiando diversas opciones de bloqueo del documento que, sin eliminar un documento firmado, impidiera el acceso al mismo, pero tampoco afectara al funcionamiento general del sistema.

2. EVIDENCIAS, SI SE HA PRODUCIDO, DE LA RETIRADA POSTERIOR DEL MENCIONADO DOCUMENTO.

El documento ha quedado bloqueado.

Al acceder al mismo, bien a través de la url de verificación o escaneo del código qrcode, el sistema responde que el documento no está accesible.

El documento no se ha eliminado, pero se ha bloqueado el acceso.

Se adjunta copia de pantalla con la respuesta del sistema al intentar acceder al documento.

3. MOTIVOS POR LOS QUE SE PRODUJO LA BRECHA DE SEGURIDAD ORIGEN DE LOS HECHOS RECLAMADOS.

El motivo que ocasionó la brecha de seguridad se debió a un uso erróneo en una utilidad en el sistema de gestión de Policías Locales (*[nnn]*) que utiliza el Ayuntamiento de Vélez Rubio.

La aplicación cuenta con una utilidad que permite generar un único documento a partir de varios informes.

Se puede observar en la documentación remitida un listado de varios documentos PDF.

El usuario puede marcar un único documento para enviar a firmar o bien marcar varios documentos para que se genere un solo informe que es unión de los documentos seleccionados y enviar a firmar, dando lugar a un informe de firma con un único CSV o QRCODE.

El usuario instructor marcó varias sanciones generando un solo documento que contenía la información de varios denunciados, aunque después separaba la información para notificar a cada ciudadano la sanción que le correspondía, pero en dicha notificación figuraba el CVS y QRCODE que llevaba al documento unión de todas las sanciones.

El acceso a través del QRCODE mostraba el documento total con la información de todos los denunciados.

Lo que se debería haber hecho:

Habría que marcar cada notificación de forma individual, para que se genere un documento para cada uno y enviarlo a portafirmas, de forma que si hay 15 notificaciones se generan 15 documentos y 15 firmas respectivamente. La URL del CSV y QRCODE son distintas para cada documento.

Todo esto se debió a una falta de formación y concienciación del problema sobre el uso de la herramienta al usuario que generó las notificaciones a los denunciados.

Con fecha 22 de septiembre de 2022, desde el Servicio de Nuevas Tecnologías de la Diputación de Almería se remitió correo electrónico al ayuntamiento de Vélez Rubio, para que en tanto se realizaban modificaciones en la aplicación, procedieran a realizar las notificaciones de las sanciones conforme se indica en el párrafo "Lo que se debería haber hecho".

4. INDICACION DE LAS DIRECTRICES Y PROTOCOLOS EN RELACION CON LA FIRMA DE DOCUMENTOS QUE PUDIERAN EXISTIR EN EL MOMENTO DE LA DIFUSION INCORRECTA.

En el momento de la difusión incorrecta del documento conteniendo acceso a información de datos personales de otros ciudadanos no existían directrices de protocolos de actuación.

La utilidad anteriormente descrita en el punto 3 sobre la facilidad de poder unir varios documentos en uno solo y poder realizar una firma de varios informes, está diseñada para facilitar la unificación de informes que no deberían contener datos personales.

No se contaba con protocolos de actuación para el incidente producido.

5. MEDIDAS QUE SE HAN TOMADO CON POSTERIORIDAD PARA EVITAR LA REPETICION DE CIRCUNSTANCIAS SIMILARES EN EL FUTURO.

Para evitar la unión de varias sanciones en un único documento, se ha desarrollado dentro del sistema de información de Policías Locales una nueva utilidad para la notificación de sanciones, de manera que el usuario podrá seleccionar a varios denunciados pero se generará un único documento para firmar, por sanción, que obligará al registro de salida individualizado con la notificación correspondiente, sin permitir que en la notificación aparezca referencia a través de códigos CSV o QRCODE a un documento general con la información de varios ciudadanos.

Se ha informado a los usuarios sobre el uso de la herramienta.

Se ha solicitado a la empresa que se ocupa del mantenimiento de la aplicación, que presente un mensaje de advertencia indicando:

"El envío masivo de varios documentos a firmar conteniendo datos personales puede dar lugar a vulnerabilidades en los derechos de protección de datos personales. No realicen envíos masivos a firma con datos personales."

Así mismo, se ha añadido al programa la acción de que quede constancia en el registro de actividad del hecho de que un usuario haya pulsado y aceptado, y por tanto dándose por sabedor del mensaje mostrado.

6. DETERMINACION DE LA ACTIVIDAD DE TRATAMIENTO AFECTADA DE LA INCIDENCIA OBJETO DE LA RECLAMACION.

Adjuntamos:

- RAT del Ayto de Vélez Rubio en la que se incluye la AT afectada por la incidencia: "POLICÍA LOCAL"

- Deber de información relacionada con la AT "POLICÍA LOCAL"

- Política de Privacidad publicada en la web del Ayuntamiento: https://www.velezrubio.es/Servicios/cmsdipro/index.nsf/contenidos.xsp?p=VelezR&ref=politica_privacidad

Lo que le traslado como Secretaria del Comité de Seguridad de la Información de la Diputación de Almería e informo de que el presente informe será remitido al Ayuntamiento de Vélez Rubio. [...]"

Se adjuntaba al escrito el registro de actividades de tratamiento de datos personales para el Ayuntamiento de Vélez Rubio (Decreto 48/2021 de 9 de febrero) y copia de la información publicada en la web del ayuntamiento en cuanto Política de privacidad y protección de datos.

Cuarto. Traslado expediente brecha de seguridad sobre mismo incidente.

El 8 de noviembre de 2022, se dio traslado a este Consejo, del expediente VS-2022/009 por violación de seguridad de datos personales notificada por el Ayuntamiento de Vélez Rubio.

En el citado escrito se indicaba:

"[...] Tras el análisis de la notificación de violación de seguridad recibida, considerando el riesgo para los derechos y libertades de las personas que implica la misma y las actuaciones llevadas a cabo desde esa entidad, se le comunica que se dado traslado de toda la documentación al Consejo a fin de lograr una mejor determinación de los hechos y circunstancias que justifiquen la tramitación, en su caso, del correspondiente procedimiento por infracción de la normativa de protección de datos personales. El motivo fundamental de dicho traslado es:

- No haber tomado las medidas de seguridad suficientes para que, una vez producida la brecha de seguridad, se minimizaran los efectos causados por la misma, toda vez que no se inhabilitó el acceso al documento difundido erróneamente. [...]"

Quinto. Evidencias incumplimiento.

El día 3 de agosto de 2023 se comprueba por el personal de este Consejo que al acceder a la herramienta de verificación de firma a través del código QR e introducir el código de verificación segura se seguía accediendo al documento conjunto con diversas notificaciones de denuncia dirigidas a diferentes personas.

Sexto. Acuerdo de inicio de procedimiento sancionador. (arts. 68 LOPDGDD; Art. 64 LPAC).

1. El 13 de septiembre 2023 el director del Consejo dictó Acuerdo de Inicio de procedimiento sancionador contra el Ayuntamiento de Vélez Rubio, con NIF *[NNNNN]*, por la presunta infracción de los artículos 5.1.c) y 32 RGPD; tipificadas en los artículos 83.5.a) y 83.4.a) RGPD; y en los artículos 72.1.i) y 73.f) LOPDGDD, y calificada a efectos de prescripción en el artículo 77.2 LOPDGDD.

2. En el mencionado acuerdo se designaba al funcionario que suscribe como Instructor del presente procedimiento sancionador, sin que se haya realizado solicitud de recusación alguna.

3. Notificado el acuerdo de inicio al órgano reclamado el 14 de septiembre 2023, éste presentó alegaciones en las que, en síntesis, manifestaba lo siguiente:

"El Ayuntamiento de Vélez Rubio, con fecha 14/09/2023 y núm. de registro de entrada *[nnn]*, remite al Comité de Seguridad de la Información de la Diputación, DPD de ese Ayuntamiento, el acuerdo de inicio de procedimiento sancionador por presunta infracción de la normativa de protección de datos personales, del Consejo de Transparencia y Protección de datos de Andalucía.

En el informe de este Comité de fecha 20 de octubre de 2022, se indicaba que el documento al que se refería el procedimiento sancionador había quedado bloqueado, ya que, al acceder al mismo, bien a través de la url de verificación o escaneo del código qrcode, el sistema responde que el documento no está accesible. El documento no se eliminó, pero se bloqueó el acceso.

En el citado informe, asimismo se exponen las medidas de seguridad adoptadas para evitar la repetición de circunstancias similares en el futuro, señalando que:

"Para evitar la unión de varias sanciones en un único documento, se ha desarrollado dentro del sistema de información de Policías Locales una nueva utilidad para la notificación de sanciones, de manera que el usuario podrá seleccionar a varios denunciados pero se generará un único documento para firmar, por sanción, que obligará al registro de salida individualizado con la notificación correspondiente, sin permitir que en la notificación aparezca referencia a través de códigos CSV o QRCODE a un documento general con la información de varios ciudadanos.

Se ha informado a los usuarios sobre el uso de la herramienta.

Se ha solicitado a la empresa que se ocupa del mantenimiento de la aplicación, que presente un mensaje de advertencia indicando:

"El envío masivo de varios documentos a firmar conteniendo datos personales puede dar lugar a vulnerabilidades en los derechos de protección de datos personales. No realicen envíos masivos a firma con datos personales."

Así mismo, se ha añadido al programa la acción de que quede constancia en el registro de actividad del hecho de que un usuario haya pulsado y aceptado, y por tanto dándose por sabedor del mensaje mostrado".

Sin embargo, tal como se recoge en el acuerdo del CTPDA de referencia, "por parte del personal agente de la autoridad de ese Consejo con fecha 3 de agosto de 2023 se podía seguir accediendo públicamente al documento con múltiples destinatarios y sus datos personales en la herramienta de verificación de firma a la que se accede a través del código QR de la reclamación original."

Se formulan las siguientes ALEGACIONES:

1º.- El Comité de Seguridad de la Información ha solicitado informe a la jefatura de la Sección de Bases de Datos y Coordinación de Aplicaciones sobre si el documento objeto de la reclamación sigue siendo accesible.

En el informe, emitido con fecha 19 de septiembre actual, que se adjunta a este escrito, se constata:

- Que desde el día 3 de octubre de 2022 se eliminó acceso a dicha petición de firmas correspondiente a los siguientes identificadores:

  [....]

- Se ha comprobado que desde ese momento la petición no ha sido modificada y que el acceso desde Verifirma de Port@firmas está prohibido.

[Se aportan imágenes que muestran que el acceso está prohibido]

- Por el técnico responsable de la aplicación se "modificó la aplicación CSV desarrollada bajo su supervisión, para permitir la inclusión de CSV que deban ser rechazados sistemáticamente como garantía adicional de revocación de acceso a documentos de dicha petición. A las *[hh:mm]* de este día confirmó que se habían hecho las modificaciones oportunas y que el acceso ya no era posible. Se ha comprobado ahora la accesibilidad y efectivamente no es posible como se puede comprobar en la imagen siguiente:

En el informe se recoge el histórico de accesos a la petición, según obra en los registros de acceso Port@firmas y se señala que "no consta acceso entre el 05-10-2022 y el 13-09-2023 tal como indican que sí han conseguido según documento del Consejo de Transparencia de Protección de Datos de Andalucía, con registro de entrada *[nnn]* de 14/09/2023 del Ayuntamiento de Vélez Rubio. Los accesos del día 14-09-2023 han sido infructuosos debido a que está prohibida la accesibilidad. No obstante se registra el acceso".

3º El Comité de Seguridad de la Información, ante la disparidad de las informaciones en relación a si continua el acceso o no al documento objeto de la reclamación y con la intención de adoptar medidas adicionales para evitar accesos de los que no tiene constancia tal y como se recoge en el acuerdo de inicio de procedimiento sancionador, ha intentado ponerse en contacto con ese Consejo para obtener información de cómo el personal agente de ese Consejo ha accedido al documento objeto de la reclamación ya que en la aplicación no ha quedado registrado el acceso del 23/08/2023. [...]"

Séptimo. Evidencias incumplimiento.

El día 6 de junio de 2024 se comprueba por el personal de este Consejo que al acceder a la herramienta de verificación de firma a través del código QR incorporado en el documento de denuncia (https://app.dipalme.org/csv/) e introducir el código de verificación segura "*[nnn]*" al que hace referencia la

reclamación, se seguía accediendo al documento conjunto con diversas notificaciones de denuncia dirigidas a diferentes personas. Se comprueba también que este CSV es distinto al que se refiere el órgano reclamado en sus alegaciones (correspondiente a la brecha notificada).

Octavo. Propuesta de resolución. (art. 89 LPAC).

1. Finalizada la instrucción del procedimiento, se procedió a realizar la correspondiente propuesta de resolución, estableciendo el plazo de diez días para la formulación de alegaciones, de conformidad con el artículo 89.2 LPACAP y en relación con el artículo 73.1 de la misma norma.

2. Notificada la propuesta de resolución a la entidad incoada el 17 de junio de 2024, ésta presentó alegaciones en las que, en síntesis, manifestaba lo siguiente:

   "[...] El Ayuntamiento de Vélez Rubio, aporta alegaciones al contenido de la misma y presenta los siguientes documentos:

   - Un informe del Comité de Protección de Datos personales, como DPD del Ayuntamiento de Vélez Rubio, sobre procedimiento sancionador del Consejo de Transparencia y Protección de Datos de Andalucía (Adjunto informe)

   - Y un informe del Jefe de Sección de Bases de Datos y Coordinación de Aplicaciones y del Jefe de Sección de Desarrollo de Aplicaciones en la que queda constancia de la inhabilitación del CSV disponible en internet (Adjunto informe).

   - Estando a fecha de hoy, la documentación acreditativa de que ha dejado de estar disponible en internet el mencionado documento con múltiples destinatarios en la herramienta de verificación de firma a la que accede a través del código QR (Adjunto pantallazo).

   También manifestar que la empresa encargada del programa "*[nnn]*", ha cambiado el diseño en la aplicación, impidiendo que pueda volver a producirse éste tipo de error humano. Adoptando el ayuntamiento las medidas correctoras. [....]"

Se adjuntaba la referida documentación:

- Copia del Informe del Comité de Protección de Datos Personales, como DPD del Ayuntamiento de Vélez Rubio, sobre procedimiento sancionador del Consejo de Transparencia y Protección de Datos de Andalucía donde, entre otras cuestiones, se indicaba:

  "[...] Como conclusiones fundamentales podemos señalar que:

  1. El DPD del Ayuntamiento de Vélez Rubio (que en ese momento era el Comité de Seguridad de la Información de la Diputación de Almería), a raíz del comunicado del CTPD de Andalucía de fecha 16 de septiembre de 2022, en el que literalmente dice "... se cierra el expediente sobre la brecha de seguridad y se abre un nuevo expediente por parte del Consejo a fin de lograr una mejor determinación de los hechos", cuando cuatro días después recibe la notificación de la apertura del

expediente RCO-2022/090, en el que no consta el CSV al que se refiere la reclamación ni datos de la persona reclamante para poder localizar el documento, considera que este nuevo expediente es el que se señala en el escrito de 16 de septiembre de 2022 que se iba abrir para una mejor determinación de los mismos hechos investigados en la brecha de seguridad.

2. De hecho, de ese nuevo expediente que se iba a abrir no se ha recibido ninguna comunicación, por lo siempre se ha considerado que los hechos eran los investigados inicialmente.

3. Es en la propuesta de resolución de procedimiento sancionador del CTPD de Andalucía, cuando por primera vez la Diputación de Almería recibe información sobre el CSV del documento objeto de la reclamación y adopta inmediatamente las medidas correctoras, tal como se ha señalado anteriormente en este informe.

4. Como se ha dicho, en el escrito de alegaciones de 27 de septiembre de 2023 se hizo la referencia respecto al CSV sobre el que se había actuado, pero, en ningún momento el CTPD de Andalucía ha puesto de manifiesto que no era ese el CSV de referencia del expediente RCO-2022/090.

5. En todos los casos, una vez que se ha tenido conocimiento de los datos necesarios para ello, el Servicio de Nuevas Tecnologías de la Diputación de Almería ha actuado con celeridad, para revocar los accesos a las notificaciones realizadas de manera irregular y para resolver, junto con la empresa que ha desarrollado la app "*[nnn]*", los problemas que habían ocasionado el error humano que ha dado lugar al posible incumplimiento de la normativa de protección de datos".

— Copia del Informe técnico acerca de procedimiento sancionador relativo al expediente 2022/ *[nnn]* por notificación masiva de denuncias a través de la aplicación *[nnn]* por el Ayuntamiento de Vélez Rubio donde, entre otras cuestiones, se manifestaba:

"[…] 2. A raíz de la brecha de seguridad comunicada por el Ayuntamiento de Vélez Rubio, se detecta el problema de privacidad que se estaba originando por el hecho de que un usuario de la aplicación no utilizara correctamente las funcionalidades de la misma:

- El usuario genera una única notificación electrónica (un solo documento con un único código CSV), las remesa de notificaciones para imprimir (notificaciones en papel) en la que el notificado iba incluido.

  Esto ocasionó que el código CSV permitiera el acceso al documento en el que se incluían notificaciones de múltiples personas con indicación de sus datos personales y hechos denunciados.

- Personal del Ayuntamiento de Vélez Rubio ponía para la firma las remesas de notificaciones como un único documento, con lo cual se generó un único CSV para notificaciones diferentes de una misma remesa.

3. Desde la Diputación de Almería se procedió a eliminar el acceso a la información del CSV, comunicado por el Ayuntamiento de Vélez Rubio, y se contactó con la empresa desarrolladora (*nnn*) para que en un principio y urgentemente generara un mensaje de alerta a los usuarios de los Ayuntamientos, para evitar que el problema se pudiera repetir.

Mientras se intervenía en el diseño de la aplicación para impedir el error humano.

Los esfuerzos del personal del Servicio de Nuevas Tecnologías, conjuntamente con el personal de la empresa encargada de tratamiento, han estado dirigidos a modificar el diseño de la aplicación.

A día de hoy, y desde principios del 2024, la aplicación no permite que los usuarios cometan los tipos de errores señalados anteriormente.

4. El día 3 de octubre de 2022 se solicita revocación de acceso a la notificación con CSV *[nnn]* firmada el día 11 de mayo de 2022, quedando ese mismo día inaccesible.

5. El día 17 de junio de 2024, a través del Comité de Protección de Datos de la Diputación de Almería, se ha recibido CSV de otra notificación masiva, firmada con fecha 6 de mayo de 2022, que no se había detectado anteriormente, y se ha procedido a revocar su acceso estando actualmente inaccesible. Esta se trata de una notificación realizada antes de los cambios introducidos en la aplicación para evitar este tipo de notificaciones.

6. La Diputación de Almería no puede identificar de forma directa las notificaciones electrónicas mal practicadas, en las que se haya producido una filtración de datos personales, ya que este es un proceso del Ayuntamiento realizado por su personal y solo puede actuar únicamente cuando se le comunique el CSV de una notificación mal realizada".

Noveno. Evidencias incumplimiento.
El día 4 de septiembre de 2024 se comprueba por el personal de este Consejo que al acceder a la herramienta de verificación de firma a través del código QR incorporado en el documento de denuncia (https://app.dipalme.org/csv/) e introducir varios de los códigos de verificación segura "*[nnn]*" que constaban en la reclamación original aportada por la persona reclamante, que ya no están disponibles.

HECHOS PROBADOS

De los documentos obrantes en el expediente y de las actuaciones practicadas, pueden considerarse como hechos probados que:

Primero. Se produjo la difusión de datos personales de un conjunto de personas mediante la verificación telemática de la firma del documento de notificación de multas de tráfico, a través de códigos QR incorporado en el documento de denuncia.

Segundo. La difusión de los datos [tanto en el caso del código QR denunciado en la reclamación como el comunicado en brecha de seguridad] se debió a la falta de medidas apropiadas que impidieran que usuarios de la aplicación de sanciones de la policía local utilizara una funcionalidad que permitía la firma

de varias denuncias en un solo documento electrónico aunque posteriormente se remitieran individualmente a cada sujeto. Aun no estando pensada dicha funcionalidad para documentos que tuvieran datos personales, la aplicación permitía usarla con estos fines; no existiendo directrices, protocolo ni formación al respecto.

Tercero. Una vez conocido el problema, se modificó la aplicación para impedir la mencionada funcionalidad y se bloqueó el acceso a los documentos electrónicos correspondientes a los QR especificados en el expediente de brecha de seguridad y los referidos en la reclamación, una vez comunicados por este Consejo.

Cuarto. El 4 de septiembre de 2024, los documentos ya no están accesibles desde el código QR de la reclamación original introduciendo el código de verificación segura señalado.

FUNDAMENTOS JURÍDICOS

Primero. Sobre la competencia.

1. De conformidad con lo previsto en el artículo 57.1 y 64.2 LOPDGDD y el artículo 43.1 LTPA en relación con el artículo 3.1 LTPA corresponde a este Consejo como autoridad autonómica de protección de datos personales y dentro de su ámbito competencial, el ejercicio de la potestad sancionadora y de los poderes previstos en el artículo 58 RGPD.

2. La competencia para la adopción de esta resolución reside en el director, conforme al art. 48.1.i) LTPA y el art. 10.3.i) Estatutos.

3. Debe destacarse a su vez que, en virtud del artículo 16.5 del Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, "*[e]l personal funcionario del Consejo, cuando realice funciones de investigación en materias propias de la competencia del Consejo, tendrá el carácter de agente de la autoridad*", con las consecuencias que de aquí se derivan para los sujetos obligados en relación con la puesta a disposición de la información que les sea requerida en el curso de tales funciones investigadoras.

4. Este procedimiento se inicia como consecuencia de una presunta vulneración de la normativa de protección de datos por parte de una entidad bajo el control del Consejo en lo que respecta al cumplimiento de dicha normativa. Por ello, en el presente caso, solo serán analizadas y valoradas aquellas cuestiones planteadas por el reclamante, en relación con la materia de protección de datos personales, que queden incluidas dentro de la esfera de responsabilidad de la mencionada entidad.

Segundo. Sobre el tratamiento de datos personales.

1. El Art. 2.1. RGPD dispone: "*[e]l presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero*".

2. El Art. 4.1 RGPD define «dato personal» como "*[t]oda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".*

   Los datos personales a los que se refiere la denuncia son los identificativos (nombre y apellidos, DNI/NIF, dirección, teléfono, firma electrónica, fecha y objeto del escrito, cargo, datos familiares, fecha y lugar de nacimiento, sexo, nacionalidad y datos relativos a infracciones administrativas (denuncias por infracciones administrativas en materia de tráfico).

3. De acuerdo con el Art. 4.2 RGPD, el tratamiento de datos personales es *"cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".*

   En este caso, el tratamiento denunciado sujeto a la normativa sobre protección de datos, que se observan en relación con los datos personales afectados es la notificación de denuncia de multas de tráfico.

   En relación a la citada operación de tratamiento realizada la entidad incoada dispone de Registro de Actividades de Tratamiento, y la misma se enmarcaría en la actividad de tratamiento *"Policía Local"*

   La finalidad de dicho tratamiento es la *"Gestión de los servicios de la Policía Local".*

4. Por último el Art. 4.7 RGPD considera responsable del tratamiento a aquella *"…autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento…"* Esta identificación del responsable de tratamiento debe entenderse completada por la concreción del *tercero* realizada en el art. 4.10 RGPD, e incluir por tanto a las "*personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable…".*

   El responsable del tratamiento es la entidad incoada, el Ayuntamiento de Vélez Rubio.

Tercero. Sobre la calificación jurídica de los hechos.

La persona reclamante denuncia la difusión de datos personales de un conjunto de personas a través de la verificación telemática de la firma del documento de notificación de multas de tráfico, a través de un código QR.

1. Preceptos infringidos.

   El artículo 5.1.f) RGPD establece el principio de "integridad y confidencialidad", por el cual los datos personales serán *"tratados de tal manera que se garantice una seguridad adecuada de los datos*

personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas".

Debe entenderse que este deber de confidencialidad tiene como finalidad evitar que se realicen filtraciones de los datos no consentidas por los titulares de los mismos. Dicho deber supone una obligación que incumbe no sólo al responsable y encargado del tratamiento sino a todo aquel que intervenga en cualquier fase del tratamiento, siendo además complementario del deber de secreto profesional.

El artículo 32 RGPD se refiere a la "seguridad del tratamiento", y en su apartado primero establece que:

> *"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*
>
> *a) la seudonimización y el cifrado de datos personales;*
>
> *b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
>
> *c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
>
> *d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento".*

En este mismo sentido, el considerando 83 RGPD señala que:

> *"A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".*

2. Consideraciones jurídicas sobre la existencia de infracción.

De la documentación que obra en el expediente, y tras la realización de las actuaciones previas de investigación, quedo acreditado que la aplicación usada para la notificación de denuncias por

infracciones de tráfico no disponía de las medidas de seguridad suficientes para evitar la difusión de los datos personales contenidos en las denuncias por infracción ya que permitía la firma en un solo documento de notificaciones dirigidas a una pluralidad de destinatarios. No parece justificado que la aplicación ofreciera la posibilidad de poder firmar en un solo documento las notificaciones remitidas a distintas personas, haciendo depender únicamente de la formación del agente la posibilidad de que se produjera una filtración de seguridad como la que se ha producido.

Por otro lado, la entidad incoada reconoció que en el momento de la difusión incorrecta del documento conteniendo acceso a información de datos personales de otros ciudadanos no existían directrices ni protocolos de actuación dirigidos a su personal en relación con la firma de documentos.

La entidad reclamada, a través de su DPD, afirmó en su informe de 20 de octubre de 2022 que:

> "El documento ha quedado bloqueado.
>
> Al acceder al mismo, bien a través de la url de verificación o escaneo del código qrcode, el sistema responde que el documento no está accesible.
>
> El documento no se ha eliminado, pero se ha bloqueado el acceso."

Sin embargo, por parte de personal agente de la autoridad de este Consejo se comprobó el 3 de agosto de 2023 que seguía siendo posible acceder públicamente al documento con múltiples destinatarios y sus datos personales en la herramienta de verificación de firma a la que que accede a través del código QR de la reclamación original.

Es cierto que la entidad incoada ha adoptado importantes medidas desde el incidente para minimizar la posibilidad de que vuelva a ocurrir lo mismo, incorporando novedades y medidas de rediseño en la aplicación para que al mandar conjuntamente a firmar las notificaciones se generen notificaciones de denuncias individuales y ello se valora muy positivamente.

Sin embargo, la entidad incoada, como responsable del tratamiento incumplió los artículos 5.1.f) y 32 RGPD al no existir medidas apropiadas para garantizar la confidencialidad de los datos en el momento de los hechos denunciados. Ello, como ya se ha mencionado, con independencia de las medidas que se tomaran con posterioridad para evitar que volviera a ocurrir. Por otro lado, en el momento del acuerdo de inicio seguía estando accesible el documento múltiple origen de la reclamación, no estando inhabilitada la URL de acceso.

3. Valoración de las alegaciones al acuerdo de inicio, pruebas practicadas o medidas provisionales.

El Ayuntamiento alegó al acuerdo de inicio que el documento con múltiples destinatarios ya no es accesible a través de la herramienta de verificación. Sin embargo, se compruebó que accediendo a través del código QR que aparecía en la denuncia en la reclamación original con el código CSV indicado, que es diferente al que menciona el Ayuntamiento en sus alegaciones, siguía pudiéndose acceder, evidenciándose que existía una confusión sobre cual es el código QR cuyo acceso se debe suprimir.

Como ya se ha reiterado, con independencia de que se hubiera impedido el acceso al documento en cuestión y se hubieran adoptado medidas con posterioridad, se produjo la vulneración de los artículos 5.1.f) y 32 RGPD.

De acuerdo con todo lo expuesto, entendemos que las alegaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

4. Valoración de las alegaciones a la propuesta de resolución, pruebas practicadas o medidas provisionales.

Efectivamente se ha producido una confusión en cuanto a las URLs objeto de la reclamación y el Ayuntamiento ha bloqueado todas las URLs que se le han indicado una vez que por parte del Consejo se le ha informado de las mismas.

Sin embargo, el objeto de este procedimiento sancionador es determinar si ha existido infracción por ausencia de medidas de seguridad en el momento de producirse los hechos que provocaron una vulneración de la confidencialidad de los datos, es decir, si exisitían las medidas de seguridad adecuadas al riesgo que hubieran impedido la vulneración de la confidencialidad de los datos. Ello, con independencia de que con posterioridad a la divulgación se bloqueara el acceso a los documentos electrónicos.

En este sentido, este Consejo, del mismo modo que reconoce el valor de las medidas adoptadas con posterioridad a los hechos, no puede obviar la circunstancia de que en el momento de los hechos no existían directrices ni protocolos de actuación en relación con la firma de documentos y se permitía notificar en un solo documento denuncias por infracciones de tráfico pertenecientes a una diversidad de personas dando lugar a la vulneración del principio de confidencialidad de datos.

Por otro lado, una vez que el Ayuntamiento fue consciente de la existencia de la brecha de seguridad ocasionada por una configuración de la aplicación que permitía que esta ocurriera y teniendo en cuenta que la falta de formación y directrices al respecto podría conllevar la existencia de otros supuestos similares (distintos incluso al referido en la reclamación), entiende este Consejo que era razonable esperar que por parte de la entidad reclamada se intentara identificar si con anterioridad o posterioridad a un caso concreto se había producido el mismo problema en otros casos, bien a través de los servicios tecnológicos que le presta la Diputación Provincial, de ser esto técnicamente posible, o bien directamente preguntando a sus propios agentes de policía local que, como usuarios de la aplicación podían revisar sus denuncias anteriores y debían forzosamente conocer el modo en el que habían actuado como usuarios de la misma. De esto modo, parece razonablemente factible haber identificado todos los casos en los que se haya producido el mismo problema, sean conocidos o no por este Consejo o hayan sido denunciados o por los afectados.

De acuerdo con todo lo expuesto, cabe señalar que las alegaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

5. Tipificación.

Los hechos atribuidos a la entidad incoada, por las razones expuestas, supone las siguientes infracciones a la normativa de protección de datos personales:

El incumplimiento de las disposiciones relativas a *"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"* del RGPD tipificada en el artículo 83.5.a) RGPD; calificada a efectos de prescripción en la LOPDGDD como infracción muy grave por vulneración sustancial del artículo 5.1.f) RGPD *"Principios relativos al tratamiento"* y, en particular, en el artículo 72.1.i) LOPDGDD:

> *"i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica.".*

Por otro lado, el incumplimiento de "*las obligaciones del responsable y del encargado a tenor de los artículos 25 a 39*" del RGPD tipificada en el artículo 83.4.a) RGPD; calificada a efectos de prescripción en la LOPDGDD como infracción grave por vulneración sustancial del artículo 32.1 RGPD *"Seguridad del tratamiento"* y, en particular, en el artículo 73.f) LOPDGDD:

> *"La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679".*

Cuarto. Sobre la identificación de la entidad responsable (art. 89.3 LPAC).

De conformidad con lo previsto en el artículo 70.1 LOPDGDD, se identifica como entidad responsable de la infracción, al Ayuntamiento de Vélez Rubio.

Quinto. Declaración de la infracción y medidas a adoptar (art. 77.2 LPAC y 58.2 RGPD).

1. El artículo 77 LOPDGDD establece el régimen sancionador aplicable a determinadas categorías de responsables o encargados del tratamiento; incluyendo, entre otros a:

> *"a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.*
>
> *[...]*
>
> *c) [...] las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.*
>
> *[...]*

En el mencionado artículo, en su apartado 2, se señala que:

"Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.[...]".

A su vez, en su apartado 3, se señala que:

"Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda."

Así, de acuerdo con el artículo 77.2 LOPDGDD, procede declarar la infracción o infracciones antes descritas.

2. Por otra parte, en relación con las medidas que proceda adoptar, el artículo 58.2 RGPD dispone que:

"Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación: [...]

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado; [...]

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición; [...]

j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional. [...]".

En el caso que nos ocupa no procede ordenar al Ayuntamiento de Vélez Rubio la adopción de medidas adicionales.

Sexto. Notificaciones y comunicaciones.

En relación con la notificación de la resolución del procedimiento sancionador, el artículo 77.2 LOPDGDD dispone que "*[l]a resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso*".

Además, el artículo 77.4 LOPDGDD señala que "*[s]e deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores*", y el 77.56 LOPDGDD, que "*[s]e comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo*".

En virtud de todo lo expuesto, el director del Consejo de Transparencia y Protección de Datos de Andalucía dicta la siguiente,

RESOLUCIÓN

Primero. Declarar las infracciones responsabilidad del Ayuntamiento de Vélez Rubio, con CIF *[NNNNN]*, por la comisión de las siguientes incumplimientos:

- Infracción tipificada en el artículo 83.5.a) RGPD y calificada a efectos de prescripción como muy grave en el artículo 72.1.i) LOPDGDD por vulneración del artículo 5.1.f) RGPD por incumplimiento del principio de confidencialidad de datos.

- Infracción tipificada en el artículo 83.4.a) RGPD y calificada a efectos de prescripción como grave en el artículo 73.f) LOPDGDD por vulneración del artículo 32.1) RGPD como consecuencia de la falta de medidas de seguridad técnicas y organizativas que garanticen la confidencialidad de los datos personales.

Segundo. Que se notifique la presente resolución al órgano infractor y a los afectados que tuvieran la condición de interesado.

Tercero. Que se comunique la presente resolución al Defensor del Pueblo Andaluz, de conformidad con lo establecido en el artículo 77.5 LOPDGDD

En consonancia con lo establecido en el artículo 50 LOPDGDD, la presente Resolución se hará pública, disociando los datos que corresponda, una vez haya sido notificada a los interesados.

Contra esta Resolución, que pone fin a la vía administrativa, cabe interponer recurso potestativo de reposición ante este Consejo, en el plazo de un mes, o interponer directamente recurso contencioso-administrativo ante el Juzgado de lo Contencioso Administrativo de Sevilla que por turno corresponda, en el plazo de dos meses, en ambos casos a contar desde el día siguiente al de su notificación, de conformidad con lo dispuesto en los artículos 30.4, 123 y 124 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en los artículos 8.3 y 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

No obstante, al tratarse de un acto en materia de sanciones, el demandante podrá elegir alternativamente interponer el citado recurso contencioso-administrativo ante el juzgado o el tribunal en cuya circunscripción tenga aquél su domicilio, siempre entendiendo esta elección limitada a la circunscripción del Tribunal Superior de Justicia de Andalucía, de conformidad con lo dispuesto en los apartados segundo y tercero del artículo 14.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Conforme a lo previsto en el art. 90.3.a) LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta ante este Consejo su intención de interponer recurso contencioso-administrativo y traslada al mismo, una vez interpuesto, la documentación que acredite su presentación. Si el Consejo no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo correspondiente o en dicho recurso no se solicitara la suspensión cautelar de la resolución, se daría por

finalizada la mencionada suspensión.

EL DIRECTOR DEL CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS DE ANDALUCÍA

Jesús Jiménez López