Junta de Andalucía

Consejo de Transparencia y Protección de Datos de Andalucía

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

Resolución	RPS-2024/031
Procedimiento Sancionador	PS-2023/030
Expediente	RCO-2020/084
Entidad incoada	Ayuntamiento de Jerez de la Frontera
Motivo de la reclamación	Posibles accesos indebidos a nnn expedientes bajo responsabilidad del Ayuntamiento
Artículo afectado	5.1.f) 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. Reclamación.

El Consejo de Transparencia y Protección de Datos de Andalucía (en adelante, el Consejo) tuvo conocimiento, a través de noticias publicadas en medios de comunicación, de una posible vulneración de la normativa de protección de datos personales como consecuencia de posibles accesos indebidos a unos nnn expedientes bajo responsabilidad del Ayuntamiento de Jerez de la Frontera por parte de dos personas empleadas municipales.

El artículo 67.1 LOPDGDD establece la posibilidad de que, ante la posible existencia de una vulneración de la normativa de protección de datos, la autoridad de control lleve a cabo de oficio actuaciones previas de investigación 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 mencionada normativa.

Segundo. Apertura de Actuaciones Previas de Investigación (arts. 65.5 y 67.1 LOPDGDD; Art. 55.2 LPAC).

En virtud del artículo 67.1 LOPDGDD, con fecha 17 de diciembre de 2020 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

En el marco de dichas actuaciones previas de investigación, el 18 de diciembre de 2020, desde el Consejo se anunció visita de inspección con objeto que desde el Ayuntamiento se aportara documentación, información y datos concretos sobre las circunstancias del acceso indebido, las consecuencias del mismo y también sobre las actividades de tratamiento afectadas.

El 23 de diciembre de 2020, tuvo lugar la visita de inspección en la sede del Ayuntamiento de Jerez de la Frontera, participando en la misma, el Jefe del Gabinete de Cumplimiento y el Jefe del Departamento de Responsabilidad Proactiva del Consejo y por parte del Ayuntamiento, la Teniente de Alcaldesa, el Teniente de Alcaldesa y una Asesora de Gobierno, sin embargo no se pudo contar con la presencia de personal informático ni del Delegado de Protección de Datos, por lo que no fue posible obtener la totalidad de la información técnica y administrativa que se tenía previsto recabar, si bien se manifestó la disponibilidad de la participación de dichas personas con posterioridad.

El Ayuntamiento expresó que el Delegado de Protección de Datos del Ayuntamiento de Jerez de la Frontera (en adelante, DPD) sería el interlocutor con el Consejo según establece la normativa reguladora y se habló de los extremadamente graves hechos ocurridos.

La visita de inspección se desarrolló según lo expuesto a continuación:

1.- Presentaciones e identificación de participantes.

2.- Descripción, por parte del Consejo, del objetivo de la visita.

3.- Cumplimentación del Anexo, en el que se recoge información sobre los siguientes aspectos:

- Actividades de tratamiento afectadas

- Determinación de responsables, DPD y encargados del tratamiento

- Descripción de los hechos

- Datos concretos

- Información sobre medidas de seguridad

- Documentación aportada (no se aporta ninguna en el momento de la visita)

4.- Consideraciones o comentarios finales.

5.- Impresión, lectura y firma del Acta.

A los efectos de completar la información en relación con los hechos investigados, y en uso de las facultades conferidas por el artículo 58.1 RGPD y los artículos 53.1 y 57 LOPDGDD, el 19 de noviembre de 2021, desde el Consejo se requirió al DPD para que remitiera información y documentación sobre las actuaciones llevadas a cabo. En concreto, se debía remitir:

- Cumplimentación de un Anexo que se adjuntaba; debiendo rellenar todos los campos incluidos en el mismo o justificar por qué no ha lugar a su cumplimentación. En el mismo se pedía la siguiente información:

  • las actividades de tratamiento afectadas

  • el responsable del tratamiento y los posibles encargados de los tratamientos o sistemas afectados

  • descripción de los hechos y circunstancias en relación con los accesos indebidos

  • datos concreto en relación con los accesos indebidos

  • medidas de seguridad existentes cuando ocurrieron los hechos e implantadas con posterioridad a los mismos

- Información sobre la situación del procedimiento judicial abierto como consecuencia de los hechos investigados, con indicación, en su caso, de las conclusiones del mismo.

- Cualquier otra información relevante o actuación llevada a cabo en relación con los hechos objeto de investigación.

En respuesta al citado requerimiento, el 1 de diciembre de 2021, tuvo entrada en el Consejo informe de la Sra. Alcaldesa del Ayuntamiento de Jerez de la Frontera donde informaba que:

> "Primero.- Respecto a la información requerida en el Anexo que nos remiten, a fecha actual no podemos remitirla, por cuanto toda la información que se solicita forma parte esencial de los autos del procedimiento judicial seguido contra las dos personas empleadas municipales que presuntamente participaron en el acceso indebido a documentos y expedientes administrativos.
>
> Segundo.- El citado procedimiento judicial se encuentra sustanciándose Diligencias Previas en el Juzgado de Instrucción nº de esta ciudad. En concreto Diligencias Previas nº nnnn.
> Tercero.- El sigilo obligado respecto a los hechos objeto de la denuncia penal seguida en el referido Juzgado, nos impide trasladarles cualquier otra información relevante".

Posteriormente, con fecha 3 de diciembre de 2021, tuvo entrada en este organismo respuesta de la DPD al referido requerimiento en la que se indicaba:

> "1. Que se remite adjunto el anexo de información requerido.
>
> 2. Que los hechos siguen en una causa judicial penal abierta y, por tanto, no disponemos hasta fecha de ulterior información al respecto.

3. Que no se han llevado a cabo nuevas acciones con respecto a los hechos mencionados en el punto tercero del anexo".

En el citado anexo, entre otras cuestiones, se señalaba que:

> "El pasado *[dd/mm/aa]* se detecta por el Ayuntamiento de Jerez de la Frontera filtración de información confidencialidad responsabilidad del ente local. Ante estos hechos se contrata a la empresa [Empresa de peritaje informático] para que realice tareas de peritaje informático con la finalidad de indagar sobre accesos a los ficheros informáticos, sin que en ningún momento realizasen un tratamiento de datos personales. La información relativa a este peritaje ha sido facilitada a este Consejo en relación al expediente RCE 2021/027.
>
> Con la ejecución de dichas investigaciones se detectó un acceso no autorizado por parte de una persona usuaria del área de *[Área]*. Ante dicho hecho el Ayuntamiento de Jerez de la Frontera presenta denuncia ante la Fiscalía que actualmente se encuentra en procedimiento judicial penal".

Cuarto. Acuerdo por el que se declara la caducidad de las actuaciones previas de investigación

En virtud de lo dispuesto en el artículo 67 LOPDGDD y en el artículo 122.4 del Reglamento de desarrollo de la LOPD (RLOPD), aprobado por Real Decreto 1720/2007, de 21 de diciembre, en vigor en todo aquello que no contradiga, se oponga o resulte incompatible con lo dispuesto en el RGPD y en la LOPDGDD, al haber transcurrido más de doce meses contados desde la fecha del acuerdo de la admisión a trámite de la reclamación, el 15 de junio de 2023, el director del Consejo dictó Acuerdo por el que se declara la caducidad de las actuaciones previas de investigación, ordenándose el archivo de las mismas y por el que se abrían nuevas actuaciones de investigación y se incorpora a las mismas la documentación que integra las actuaciones previas de investigación declaradas caducadas.

Quinto. Sobre las segundas Actuaciones Previas de Investigación

En el marco de dichas actuaciones y en uso de las facultades conferidas por el artículo 58.1 RGPD y el artículo 57 LOPDGDD, así como por lo dispuesto en el artículo 36 LOPDGDD, el 19 de junio de 2023, desde el Consejo se requirió al DPD para que remitiera información y documentación relativa a los hechos objeto de la reclamación y, en su caso, sobre las actuaciones llevadas a cabo en relación con la misma. En concreto, se debía remitir:

1. Determinación concreta de la actividad de tratamiento relacionada con la reclamación e identificación del responsable de dicho tratamiento, así como de los posibles encargados del tratamiento que pudieran tener relación directa con el objeto de la reclamación.
2. Copia del registro de actividades de tratamiento (en adelante RAT) relativo a la mencionada actividad, con los datos exigidos por el artículo 30 RGPD y su base legal.
3. Copia, en su caso, de las medidas, normas, procedimientos, reglas existentes en el momento de los hechos objeto de la reclamación sobre el modo en que se deben tratar los datos con el fin de garantizar la confidencialidad de los mismos.
4. A la vista de la situación reclamada, copia, en su caso, de las medidas adoptadas por el responsable para evitar que se produzcan incidencias similares en el futuro. En especial, las medidas que garanticen la confidencialidad de la documentación que contenga datos personales, evitando el posible acceso a los mismos por parte de terceros. En su caso, fecha de adopción de las citadas medidas.

Sin embargo, este Consejo no recibió respuesta al respecto.

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

1. El 28 de julio de 2023, el director del Consejo dictó Acuerdo de Inicio de procedimiento sancionador contra el Ayuntamiento de Jerez de la Frontera, con NIF *[NNNNN]*, por la presunta infracción del artículos 5.1.f) RGPD, tipificada en el artículos 83.5.a) RGPD, y calificadas a efectos de prescripción en el artículo 72.1.a) LOPDGDD.

2. Notificado el acuerdo de inicio a la entidad incoada el 28 de julio de 2023, ésta presentó alegaciones en las que, en síntesis, manifestaba lo siguiente:

> "[...] **En primer lugar**, que el DPD del Ayuntamiento de Jerez de la Frontera no tuvo constancia de la entrada por registro de ningún requerimiento de información a petición de éste Consejo motivo por el cuál no fue atendido probablemente por el cambio político y organizativo existente en fecha 16 de junio de 2023 en la corporación.
>
> **En segundo lugar**, que los datos personales afectados por la reclamación que da origen al presente procedimiento hacen referencia al tratamiento "Recursos Humanos" bajo responsabilidad del Ayuntamiento de Jerez de la Frontera como se informo en fecha 10 de mayo de 2021.
>
> **En tercer lugar,** que el Registro de las Actividades del Tratamiento (RAT) si se encuentra publicado en la a través del aviso legal y política de privacidad de la web institucional: https://transparencia.-jerez.es/fileadmin/Documentos/Transparencia/seguridad/doc/RAT.pdf
>
> **En cuarto lugar,** el único encargado de tratamiento relacionado con la reclamación que da origen al presente procedimiento es la empresa [Empresa de peritaje informático] sobre la cual ya se informó debidamente en su momento facilitando, a petición de éste Consejo en fecha 7 de septiembre de 2021, el debido acuerdo de encargado de tratamiento suscrito con el Ayuntamiento. La finalidad del servicio llevado a cabo por ésta fue el peritaje informático a los ordenadores de ambos trabajadores relacionados con la reclamación original.
>
> **En quinto lugar,** que el procedimiento judicial penal que derivo de las acciones de ambos trabajadores se encuentra aún abierto a falta de poder facilitar, por el momento, más información en relación al mismo más allá del ya facilitado anexo a éste Consejo en fecha 3 de diciembre de 2021.
>
> **En sexto lugar,** que las medidas de seguridad implantadas por la organización desde la fecha de lo acontecido son las listadas seguidamente:
>
> • La contratación de una plataforma de concienciación en ciberseguridad para 1500 empleados municipales la cual dará inicio durante el próximo mes de septiembre.
>
> • El envío de píldoras mediante correo electrónico a los empleados municipales bajo el lema "La seguridad es cosa de todos".
>
> • La realización de sesiones formativas y de concienciación generales y específicas en materia de protección de datos a las diferentes direcciones de la corporación.
>
> • La inclusión de un espacio en la intranet municipal con recomendaciones y buenas prácticas en el uso de recursos TIC:
>
> • Aprobación de la Política de Seguridad de la organización y constitución del Comité de Seguridad para el Esquema Nacional de Seguridad (ENS)

• Desarrollo de Políticas, Normativas y Procedimientos de seguridad dentro del marco del ENS (pendientes de aprobación).

En último lugar, a pesar de las medidas implantadas o en estado de implantación, los accesos indebidos a documentos y expedientes administrativos fueron a tenor de la **puesta a disposición de manera voluntaria de las credenciales de acceso** de una persona con autorización para acceder a los susodichos a otra que no disponía de dicha autorización. Que a falta de poder aplicar las medidas de **doble factor de autenticación**, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad no establece la obligatoriedad de dicha medida a excepción de que se trate de accesos a través de conexiones VPN (no sería aplicable en el supuesto que da origen al presente procedimiento). Que, aun habiendo existido dicha medida con anterioridad a dichos accesos indebidos, **no hubiera podido evitarse** dado, reiteramos, la voluntariedad con la que se facilitaron las credenciales de acceso de un usuario a otro. [...]".

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 7 de junio de 2024, ésta no presentó alegaciones.

HECHOS PROBADOS

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

Primero. Que en agosto de 2020 se detectó por el Ayuntamiento de Jerez de la Frontera la filtración de información confidencial por posibles accesos indebidos al Sistema Informático Municipal con datos personales de ciudadanos, usuarios, empleados, proveedores, clientes, menores y personas especialmente vulnerables por parte de dos *personas empleadas municipales adscritas al Servicio [Servicio]*.

Segundo. Que el propio Ayuntamiento lo denunció ante la Fiscalía y se encuentra en procedimiento judicial penal, lo que ofreció indicios suficientes de que se produjo un incidente de seguridad ya que se permitió el acceso por terceros a datos personales.

Tercero. No ha quedado acreditado que la entidad incoada hubiera adoptado suficientes medidas técnicas y organizativas con el fin de garantizar la confidencialidad de los datos personales.

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 per-

sonales 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".*

   De acuerdo con las anteriores definiciones, y en relación al caso que nos ocupa, los datos identificativos, de contacto, credenciales de acceso, datos de localización, perfiles, datos económicos o financieros, datos sobre condenas e infracciones penales y datos relativos a categorías especiales de datos de ciudadanos, usuarios, empleados, proveedores, clientes, menores y personas especialmente vulnerable, han de considerarse datos personales a los que se realiza un tratamiento. Por consiguiente, tanto los datos personales tratados como el tratamiento que se realice de los mismos han de someterse a lo establecido en la normativa sobre protección de datos personales.

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".*

La operación concreta que se observa es el posible acceso indebido a datos personales por parte de dos empleados del Ayuntamiento.

En relación a la operación de tratamiento realizada la entidad incoada dispone de Registro de Actividades de Tratamiento, la misma se enmarcaría según el DPD en la actividad de tratamiento "Recursos Humanos"[1]

La finalidad declarada del tratamiento, tal y como se declara en el Registro de Actividades de Tratamiento es *"Recursos humanos, Gestión de nóminas, Gestión de nóminas (discapacitados), Prevención de riesgos laborales, Fines de interés público basados en la legislación vigente".*

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 el Ayuntamiento de Jerez de la Frontera.

Tercero. Sobre la calificación jurídica de los hechos.

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.

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, ha quedado acreditado que en agosto de 2020 se detectó por el Ayuntamiento de Jerez de la Frontera la filtración de información confidencial por posibles accesos indebidos al Sistema Informático Municipal con datos personales de ciudadanos, usuarios, empleados, proveedores, clientes, menores y personas especialmente vulnerables por parte de d*os personas empleadas municipales adscritas al Servicio [Servicio]*, habiendo presentado el propio Ayuntamiento denuncia ante la Fiscalía y encontrándose actualmente en procedimiento judicial penal, lo que ofrece indicios suficientes de que se produjo un incidente de seguridad en el ámbito del responsable del tratamiento con quebrantamiento del principio de confidencialidad puesto que se permitió el acceso por terceros a datos personales.

1 *https://transparencia.jerez.es/fileadmin/Documentos/Transparencia/seguridad/doc/RAT.pdf*

Aunque el artículo 32 RGPD no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas, éstas deberán garantizar la confidencialidad de los datos.

Desde este organismo se requirió al órgano reclamado en varias ocasiones para que aportara Información sobre las medidas de seguridad, normas, procedimientos o reglas implementadas en el Ayuntamiento de Jerez en el momento en que ocurrieron los hechos, así como detalle de las medidas adoptadas con posterioridad para evitar posibles incidencias similares en el futuro. Sin embargo, este Consejo consideró insuficientes las medidas existentes a las que se refería el Anexo remitido y no se recibió contestación respecto a las implantadas con posterioridad.

El Ayuntamiento incoado se ha amparado en la existencia de un deber de sigilo a consecuencia del proceso judicial abierto. Sin embargo, entiende este Consejo que este deber de sigilo no tendría por qué afectar a la información sobre las medidas de seguridad establecidas, independientemente de las circunstancias concretas del caso sometido a investigación judicial.

Por consiguiente, en relación con los hechos objeto de la reclamación, y en tanto en cuanto, por una parte, se ha producido un acceso inadecuado a datos personales por parte de empleados, y por otra, no se ha aportado evidencia alguna ni ha quedado acreditado que el órgano reclamado disponga de medidas o procedimientos de seguridad suficientes sobre el modo en que se tratan los datos de carácter personal, evitando el posible acceso a los mismos por parte de terceros, el Ayuntamiento de Jerez de la Frontera, como responsable del tratamiento, incumplió, por las circunstancias expuestas anteriormente, el mencionado artículo 5.1.f) RGPD por vulneración del principio de confidencialidad como consecuencia de los accesos indebidos a datos personales por la falta de medidas técnicas y organizativas.

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

La entidad incoada alega la implementación de distintas medidas de seguridad desde la fecha de lo acontecido. En concreto:

- La contratación de una plataforma de concienciación en ciberseguridad para 1500 empleados municipales.

- El envío de píldoras mediante correo electrónico a los empleados municipales bajo el lema “La seguridad es cosa de todos”.

- La realización de sesiones formativas y de concienciación generales y específicas en materia de protección de datos a las diferentes direcciones de la corporación.

- La inclusión de un espacio en la intranet municipal con recomendaciones y buenas prácticas en el uso de recursos TIC.

- Aprobación de la Política de Seguridad de la organización y constitución del Comité de Seguridad para el Esquema Nacional de Seguridad (ENS)

- Desarrollo de Políticas, Normativas y Procedimientos de seguridad dentro del marco del ENS (pendientes de aprobación).

Sin embargo, este Consejo, a pesar de reconocer el esfuerzo realizado por la entidad incoada, entiende que estas alegaciones ponen de manifiesto que en el momento de producirse los hechos no existían las medidas de seguridad apropiadas en lo referente al Esquema Nacional de Seguridad, en adelante ENS, puesto que la obligación de atener los sistemas adecuados al ENS ya era exigible el 5 de noviembre de 2017 de conformidad con la Disposición Transitoria Única del 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.

Por lo tanto, la obligación de disponer de una política y comité de seguridad TIC a la que se refería el artículo 11 y la medida "3.1 Política de seguridad [org.1]." del Anexo II del citado Real Decreto 3/2010, de 8 de enero, ya existía con varios años de anterioridad a producirse los accesos indebidos.

Por otro lado, la aprobación de una política de seguridad TIC y la creación de un comité de seguridad TIC es solo el primer paso para la adecuación al ENS, actualmente regulado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Dicha adecuación requerirá otros pasos para su culminación, como la aprobación de Políticas, Normativas y Procedimientos de seguridad, de la Declaración de Aplicabilidad de las medidas de seguridad, previos los oportunos análisis de riesgo o de la Declaración de Conformidad para los sistemas de categoría Básica o Certificación de Conformidad para los sistemas de categoría Media y Alta, o bien los requisitos exigidos para perfiles de cumplimiento específicos.

Por tanto se consideran insuficientes las medidas adoptadas y considera necesario que el Ayuntamiento de Jerez de la Frontera culmine la adaptación de sistemas al ENS con el fin de adoptar las medidas de seguridad técnicas y organizativas necesarias para dar cumplimiento al principio de confidencialidad y evitar los accesos indebidos a datos personales por parte de terceros.

En este punto debemos recordar que la obligación de adoptar medidas de seguridad adecuadas al riesgo no es una obligación de resultado sino de medios, tal y como queda reflejado en varias sentencias y pronunciamientos de autoridades de control, por todas la sentencia del tribunal supremo STS 543/2022, de 15/02/2022, en la que en su fundamento jurídico cuarto se señala que:

> *"Ya hemos razonado que la obligación que recae sobre el responsable del fichero y sobre el encargado del tratamiento respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos de carácter personal no es una obligación de resultado sino de medios, sin que sea exigible la infalibilidad de las medidas adoptadas. Tan solo resulta exigible la adopción e implantación de medidas técnicas y organizativas, que conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado."*

Por consiguiente, y de acuerdo con lo expuesto el Ayuntamiento no había adoptado e implantado medidas técnicas y organizativas adecuadas para minimizar el riesgo de que se produjeran los mencionados accesos indebidos, vulnerando así el principio de confidencialidad e integridad.

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 suficientes.

4. Tipificación.

Los hechos atribuidos a la entidad incoada, por las razones expuestas, supone la siguiente infracción 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.a) LOPDGDD:

> *"El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 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 Jerez de la Frontera.

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.*
>
> *d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.*
>
> *e) Las autoridades administrativas independientes.*
>
> *[...]*
>
> *g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.*

h) Las fundaciones del sector público.

i) Las Universidades Públicas.

j) Los consorcios.

k) Los grupos parlamentarios de […] las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

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. […]".

Para la determinación de las posibles medidas a adoptar y del plazo para adoptarlas hay que tomar en consideración que se necesita un plazo suficiente para la aplicación de las medidas de se-

guridad previstas en el ENS exige implementar un sistema de gestión permanente de la seguridad y dedicar los recursos suficientes para ello.

Para valorar la duración de este plazo se ha tenido en cuenta que la Disposición transitoria única del 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, en el que se aprobó la obligatoriedad de la aplicación del ENS a los sistemas de información de las administraciones públicas concedió un plazo de veinticuatro meses para adaptar dichos sistemas a lo dispuesto en el mismo.

En el caso que nos ocupa procede ordenar al Ayuntamiento de Jerez de la Frontera que:

Remita al Consejo, en el plazo máximo de veinticuatro meses tras la notificación de la presente resolución, la documentación acreditativa de haber aplicado a los tratamientos de datos personales responsabilidad de esa entidad las medidas de seguridad que correspondan de las previstas en el ENS, de conformidad con lo establecido en Disposición adicional primera LOPDGDD, para lo cual deberá realizar un análisis de riesgo conforme al artículo 24 RGPD y, en los supuestos del artículo 35 RGPD, una Evaluación de impacto relativa a la protección de datos.

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 la infracción responsabilidad del Ayuntamiento de Jerez de la Frontera, con CIF *[NNNNN]*, por la comisión de la siguiente infracción:

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

Segundo. Ordenar al Ayuntamiento de Jerez de la Frontera en relación con las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido:

Remita al Consejo, en el plazo máximo de veinticuatro meses tras la notificación de la presente resolución, la documentación acreditativa de haber aplicado a los tratamientos de datos personales responsabilidad de

esa entidad las medidas de seguridad que correspondan de las previstas en el ENS, de conformidad con lo establecido en Disposición adicional primera de la LOPDGDD, para lo cual deberá realizar un análisis de riesgo conforme al artículo 24 RGPD y, en los supuestos del artículo 35 RGPD, una Evaluación de impacto relativa a la protección de datos.

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

Cuarto. 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.

El incumplimiento de esta resolución podría comportar la comisión de la infracción considerada en el artículo 72.1.m) LOPDGDD, sancionable de acuerdo con el artículo 58.2 RGPD.

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