- **Expediente N.º: PS/00028/2022**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: ***A.A.A.***,(en adelante, el reclamante) con fecha 31/03/2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **AYUNTAMIENTO DE GETAFE** con NIF ***P2806500A*** (en adelante, el reclamado). Los motivos en que basa la reclamación son los siguientes:

El reclamante señala que al acceder en la sede electrónica del reclamado al supuesto documento *"*****DOCUMENTO.1** Resolución de convocatoria de sesión extraordinaria del Ayuntamiento Pleno a celebrar el ***FECHA.1"* apunta a un fichero excel https://sede.getafe.es/portalGetafe/sede/RecursosWeb/***(...)***), "*que una vez abierto, contiene nombres y apellidos, dirección, DNIs, fechas de nacimiento y matriculas y fecha matriculación de vehículos*."
Manifiesta igualmente haber interpuesto queja por este motivo al propio reclamado el 31/03/2021, aporta copia.

Aunque hay 36 registros, la gran mayoría figuran repetidos una o dos veces, en total: (…) personas

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD**),** se dio traslado con fecha de *****FECHA.2** de dicha reclamación al reclamado en el marco del procedimiento E/04923/2021, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de diversas cuestiones. En el envío se informaba del documento expuesto y la URL que alojaba el fichero y se solicitaba diversa información.

No consta respuesta al traslado, que fue notificado electrónicamente, figurando: "*fecha de aceptación : 04/05/2021 12:34:05*".

TERCERO: Con fecha 31/06/2021, por aplicación del artículo del artículo 65.5 de la LOPDGDD, prosigue la tramitación de la reclamación.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

-Con fecha 10/09/2021, se dirige desde la AEPD un requerimiento de información por vía electrónica al objeto de recabar mayor detalle sobre los hechos reclamados. Según reporte del "*Servicio de Notificaciones Electrónicas y de Dirección Electrónica Habilitada de la FNMT-RCM*", con fecha *****FECHA.3**, se produce el rechazo automático del requerimiento, tras haber transcurrido diez días naturales desde su puesta a disposición.

Con fecha de ***FECHA.4, se reitera el requerimiento anterior, esta vez por vía postal. Esta vez, tal y como acredita la confirmación de recepción de la notificación expedida por la aplicación "*Carpeta Ciudadana*", el reclamado accedió a la misma el día *****FECHA.4**. No se atendió la petición en el plazo otorgado.

-El día 1/12/2021, se accede al apartado correspondiente a la "*Consulta de Actas de Plenos*" de la sede electrónica del reclamado. Dentro del listado de sesiones, se consulta la correspondiente al día ***FECHA.1 por ser la referida por el reclamante. El resultado de esta prueba, incorporada al expediente a través de la "*Diligencia Referencias*", no redirecciona al listado referido por el reclamante, sino a la efectiva convocatoria del citado pleno, (https://sede.getafe.es/portalGetafe/sede/RecursosWeb/(...)).

-A continuación, el mismo día 1/12, se accede directamente a través del navegador a la dirección electrónica facilitada por el reclamante en la que supuestamente se incorporaba el citado listado de datos personales, https://sede.getafe.es/portalGetafe/sede/RecursosWeb/***(....)*** y se descarga la "*hoja excel*" a la que se tiene acceso y se incorpora como objeto asociado del expediente. "*Dado que el sistema SIGRID no permite la incorporación de documentos en Excel como anexos a las diligencias, se convierte a formato pdf y se adjunta a la presente diligencia. La hoja, titulada "SolicitudConvenioFEMP*" en la que se listan treinta y seis registros con los siguientes campos: "*Código*", "*Nombre*", "*Apellido 1*", "*Apellido 2*", "*Doc_Identificador*" NIF, "*Fecha_Nacimiento*", "*Tipo_Vía*", "*Nombre_Vía*", "*Nº*", "*Bloque*", "*Portal*", "*Escalera*", "*Planta*", "*Puerta*", "*Km*", "*Hm*", "*Pueblo*", "*Código_Postal*", "*Tipo Registro*", "*Matrícula*", "*Fecha_Matriculación*", "*Cotitulares*", "*Impresion*", "*Observaciones*", "*Fecha_Resolucion*", "*Resolucion*", "*Descripcion*". Los datos personales que parecen advertirse en dicho listado son: nombre, apellidos, dirección, fecha de nacimiento, número de identificación fiscal, NIE, matrícula del vehículo, y fecha de matriculación.

QUINTO: Con fecha 25/01/2022, se recibe escrito del reclamado, que manifiesta en respuesta a requerimiento información E/7831/2021:

- "*Esta entidad no ha remitido la información en el plazo requerido, dado que en dicho período hubo una transición de responsabilidades en materia de protección de datos entre el Comité de Seguridad de la Información, órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información, y la actual Delegada de Protección de Datos cuya toma de posesión tuvo lugar el pasado 1/10/2021".*

-El 31/03/2021, en la sede electrónica municipal, área correspondiente al tablón de anuncios y edictos electrónico, se procedió a publicar desde la unidad de ***DEPARTAMENTO.1, un contenido referido a la Resolución de convocatoria de sesión extraordinaria del Ayuntamiento, Pleno, a celebrar el ***FECHA.1. Como consecuencia de un error humano, involuntario y accidental, se anexó el recurso informativo incorrecto, y en vez de anexar el pdf correspondiente a la mencionada resolución, se anexó una hoja

de cálculo interna y temporal en la que aparecían datos identificativos y personales de (…) ciudadanos. Los datos comprometidos son "*nombre, apellidos, DNI, dirección postal*". "*La información que pudiera haber sido accedida por terceros podría ocasionar un daño a los afectados, pero inicialmente no se observa un perjuicio grave*."

Al recibir una queja ese día, ese mismo día, que era el mismo día de la publicación, se subsanó desde ***DEPARTAMENTO.1 con la retirada del documento y la corrección del incidente. El 22/04/2021, se remitió contestación a la queja, dando por cerrado el expediente.

-En cuanto a las acciones tomadas para solucionar el incidente y minimizar su impacto, manifiesta que el mismo (…), sustituyó el documento excel por el documento pdf de la sesión extraordinaria del Ayuntamiento.

Dado que la publicación de contenidos se encuentra descentralizada, se remitió un recordatorio a las unidades finalistas en el que se insta a realizar una "*revisión cruzada*" entre iguales, asegurando así que cada publicación es revisada por una persona del departamento distinta a la que realiza la actualización o publicación en la web o sede corporativa municipal.

-En cuanto a las medidas de seguridad de los tratamientos de datos personales adoptadas con anterioridad al incidente, manifiesta:

a) Las contenidas en el anexo dos de medidas de seguridad del Real decreto 3/2010 de 8/01, por el que se regula el esquema Nacional de Seguridad (ENS) en el ámbito de la administración electrónica.

b) En el ámbito de gestión y publicación de contenidos:

-Aplicación de gestión administrada según perfiles y departamentos.

-Los contenidos a publicar se realizan en soporte PDF conforme la "*instrucción corporativa de publicación*".

-Se dispone de los contenidos publicados, despublicados y restringidos con "*logs de acceso*".

Añade que el incidente es un error en un procedimiento manual lo que impide su repetición por motivos de automatización.

-La actividad de tratamiento de datos personales y denominada *SEDE ELECTRÓNICA*, dada la naturaleza de los datos, alcance, contexto y fines se ha considerado que no entraña un alto riesgo para los derechos y libertades de las personas físicas, por lo que no se cuenta con estudio de evaluación de impacto en materia de Protección de Datos.

Aporta copia del registro de actividades de tratamiento *SEDE ELECTRÓNICA.*

-En cuanto a si la violación de seguridad fue notificada a los afectados, manifiesta que el mismo día que se tuvo conocimiento de la situación que fue el día de la publicación del

contenido, se realizó la corrección del incidente y no se ha procedido a notificar la situación a los afectados,

-En cuanto a si la violación de seguridad ha sido notificada a la autoridad de control antes de que transcurrieran 72 horas desde que sucediera, manifiesta que no remitió información en ese plazo, dado que en dicho periodo hubo una transición de responsabilidades en materia de Protección de Datos entre el "*Comité de seguridad de la información*", órgano consultivo y estratégico para toma de decisiones en materia de seguridad de la información y la actual "*Delegada de Protección de Datos*" cuya toma de posesión tuvo lugar el 1/10/2021. También señala que "*la información que pudiera haber sido accedida por terceros podría ocasionar un daño a los afectados, pero inicialmente no se observa un perjuicio grave*."

-En cuanto a las medidas adoptadas para que no se vuelva a producir un incidente similar en el futuro, manifiesta que han actualizado la instrucción de publicación de contenidos corporativa, instando a las unidades a realizar la "*revisión cruzada*".

Finalmente, manifiestan que en el momento de realizar este informe, el departamento de informática ha revisado todo el contenido informativo almacenado y publicado tanto en la web como en la sede municipal, no habiéndose encontrado ningún recurso ni en cuyo contenido haya datos de carácter personal.

SEXTO: Con fecha 4/04/2022, la Directora de la AEPD acordó:

"*PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a AYUNTAMIENTO DE GETAFE, con NIF P2806500A, por las presuntas infracciones del RGPD, artículos:*

-5.1.f), de conformidad con el artículo 83.5.a) del RGPD, tipificada en el artículo 72.1 a) de la LOPDGDD.

-32, de conformidad con el artículo 83.4.a) del RGPD, tipificada en el artículo 73.f) de la LOPDGDD.

-33, de conformidad con artículo 83.4.a) del RGPD, tipificada en el artículo 73.r) de la LOPDGDD."

"… a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de apercibimiento, sin perjuicio de lo que resulte de la instrucción."

Recibido el acuerdo, no se presentaron alegaciones.

SÉPTIMO: Con fecha 23/06/2022, se inicia un periodo de práctica de pruebas, dando por reproducidos a efectos probatorios, la reclamación interpuesta y su documentación, los documentos obtenidos y generados durante la fase de admisión a trámite de la reclamación, y el informe de actuaciones que forman parte del procedimiento E/07831/2021.

Asimismo, se da por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio del procedimiento sancionador referenciado,

presentadas por el reclamado y la documentación que a ellas acompaña.

Se solicita al reclamado, informe o aporte la siguiente información dirigida a la verificación y comprobación de las medidas existentes en el momento de suceder los hechos:

a) En el informe de actuaciones previas figura que "*El día 1/12/2021 se accede por el inspector en fase de actuaciones previas al apartado correspondiente a la "Consulta de Actas de Plenos" de la sede electrónica del reclamado. Dentro del listado de sesiones, se consulta la correspondiente al día ***FECHA.1. El resultado de esta prueba, incorporada al expediente a través de la "Diligencia Referencias" no redirecciona al listado referido por el reclamante sino a la efectiva convocatoria del citado pleno.*

A continuación, el mismo día 1/12, se accede directamente a través del navegador a la dirección electrónica facilitada por el reclamante https://sede.getafe.es/portalGetafe/sede/RecursosWeb/(...). El resultado de esta prueba, incorporada al expediente a través de la "Diligencia Referencias", es el acceso a un documento en formato Excel que contiene una hoja titulada "SolicitudConvenioFEMP" Los datos personales que parecen advertirse en dicho listado son: nombre, apellidos, dirección, fecha de nacimiento, número de identificación fiscal, matrícula del vehículo, y fecha de matriculación."

Se solicita explique el motivo por el que no verificaron el acceso desde la url en navegador (tras indicar que al recibir la queja (…) solucionaron la cuestión), considerando que el 1/12/2021 el inspector nuevamente accedió al contenido del listado tecleando en el navegador la dirección que originariamente consiguió el reclamante (https://sede.getafe.*es/portalGetafe/sede/RecursosWeb****(...).***

Con fecha 7/07/2022, el reclamado manifiesta *que "el contenido se encontraba accesible desde el área de la web denominado "consultas de actas de Plenos" pero también en "tablón de anuncios". "La publicación concreta del contenido de la Convocatoria Extraordinaria de la Sesión Plenaria de fecha ***FECHA.1, se realizó desde el ***DEPARTAMENTO.2, quién se encarga de la publicación de estos contenidos en el "Tablón de Anuncios" Municipal en Sede electrónica.*

"R*ecibida la queja, la tramitación y contestación de la misma fue realizada por parte de la unidad de ***DEPARTAMENTO.1 (unidad responsable del contenido (…). Esta unidad remitió la solicitud de eliminación de la información al ***DEPARTAMENTO.2, unidad que desvinculó el contenido objeto de queja y que vinculó el contenido correcto y referente a la convocatoria de la sesión en formato PDF. Una vez recibida la contestación en ***DEPARTAMENTO.1 por parte del ***DEPARTAMENTO.2 con la comunicación de la corrección de la incidencia, comprobó (haciendo únicamente uso de las opciones de navegación del portal, la efectiva ausencia de dicho contenido), dando por cerrada así la incidencia y cursando la contestación a la queja dando así por cerrado el expediente*."

"*En la resolución de la queja intervinieron dos unidades no especializadas en la gestión de contenidos, por lo que la verificación efectiva del borrado mediante el acceso a la URL no se realizó*."

a) Acrediten la fecha en que es retirado o imposibilitado el acceso a través del navegador, de https://sede.getafe.es/*portalGetafe/sede/RecursosWeb****(...).***

"*El documento fue borrado con fecha 24/01/2022, con la intervención de la Unidad de Informática, verificando el contenido de la URL, y la eliminación de la mencionada hoja de cálculo en el gestor de contenidos municipal, momento en el que se realizó la formación y explicación de lo sucedido a esta unidad y a los recursos encargados del uso del gestor de contenidos. El detalle técnico de lo sucedido es que no se procedió al borrado del recurso, sino que se desvinculó del documental al que se encontrada relacionado, de manera que el documento se quedó "huérfano" en el gestor, y por tanto, aunque no accesible siguiendo la ruta de navegación en el portal, si desde la URL y por tanto internet*."

"*Se procedió a realizar una formación "in situ" así como a realizar por parte de Protección de Datos una instrucción que mejora de forma operativa las garantías en fase de publicación de contenidos sobre todo de aquellos especialmente sensibles como los que contienen datos personales. Esta instrucción es aplicable tanto en la publicación de contenidos de web municipal como en los de la sede".*

b) Informen sobre detalles del listado, ¿para que se usaba?, ¿en qué fecha fue confeccionado y hasta que fecha se conserva?¿qué unidad lo gestionaba? ¿Si se cedían los datos a otra/s unidad/es?, y ¿si esos datos se tenían que publicar por algún motivo al público? o si era un archivo de trabajo, ¿a quién se podía comunicar?

Manifiesta que "*El listado es un documento de trabajo temporal en el que se recogen por parte del ***DEPARTAMENTO.2 todos los datos referentes a solicitudes de cambio de domicilio de titulares de vehículos, y cuya información de partida son las solicitudes recibidas en el Registro General de Entrada municipal (tanto en su asistencia presencial como electrónica). La fecha de confección del documento corresponde a la semana de la publicación ya que el código de los registros de entrada determina la temporalidad del mismo. Este fichero se elabora semanalmente y tiene por objeto su remisión directa a la Jefatura Provincial de Tráfico y es borrado una vez que se tiene el ok del proceso de carga de dicha entidad. La plantilla inicial fue proporcionada por la Jefatura de Tráfico, pudiendo contener como metadatos elementos como la fecha creación, que no se corresponde con 2020. La entidad que trata y gestiona ese documento es la misma que publicó por error, el ***DEPARTAMENTO.2."*

c) Estructura de la sede electrónica en cuanto a publicación de documentos con datos personales, ¿qué documentos se han de exponer, en qué sección.?

Aporta impresión de pantalla de "*bienvenida a la sede electrónica*" figurando el apartado "*tramites y registros*" encabezado por "*catálogo de tramites"*, en la sección "*Servicios*" está: "*Oficina virtual*", "*solicitudes electrónicas*", "*pagos recibos*" "*autoliquidaciones, tributos y pagos*", "*expedición de documentos*", "*cita previa*" y "*Oficina presencial* ". En el apartado: "*Te puede interesar*", figura entre otros el apartado de consultas y de Plenos, de Actas de juntas de Gobierno. En la parte derecha figuran pestañas temáticas como "*perfil del contratante*" "*portal de transparencia*", "*tablón de anuncios*".

Expone el reclamado los espacios donde puede haber datos de carácter personal. Añade que existen contenidos y servicios que requieren identificación previa.

d) ¿Qué unidad es la encargada de exponer en la sede para el público las convocatorias de sesiones del Pleno Ayuntamiento?, y si dentro de dicha unidad lo hace siempre la misma persona y si esa persona o personas ha/n recibido formación sobre protección o instrucción del protocolo corporativo de publicación de datos, o instrucciones escritas si las

hay sobre la labor a desempeñar. Lo mismo para la unidad que gestionaba el documento de listado hoja titulada "*SolicitudConvenioFEMP*".

Responde que la publicación de convocatorias se realiza por dos unidades, ***DEPARTAMENTO.1 que publica en la sede las actas de Plenos, en "consultas de actas de Plenos", ***DEPARTAMENTO.2 que publica también en la sede, en el "*tablón de anuncios*". Aparecen publicadas en las dos áreas. (…), indicando que todas las personas han recibido formación sobre protección de datos.

Sobre la existencia de instrucción o protocolo de protección de datos de carga clasificación y publicación de contenidos, responde que "si*, inicialmente se contaba con un manual, guía y procedimiento de carga, clasificación y publicación de contenidos, y posteriormente al incidente se elaboró una instrucción en la que se insta a una revisión cruzada entre iguales, asegurando así que cada publicación es revisada por una persona del departamento distinta a la que realiza la actualización/publicación en la web / sede corporativa. - Todos estos datos aplican a ambas unidades."*

e) En cuanto a la hoja titulada: "*SolicitudConvenioFEMP*" que contenía el listado de las (…) personas, ¿qué relación existía entre las personas con esa administración para que figuraran los datos personales en dichos registros, que tipo de vinculo o actividad les relacionaba?

Manifestaron que son titulares de vehículos inscritos en el municipio y que han solicitado cambio de dirección, la categoría de datos es de "*ciudadanos*".

f) Registro de actividades de tratamiento aplicable al listado hoja titulada "*SolicitudConvenioFEMP*", y motivos que justifican el tratamiento de NIF, nombre y apellidos, matricula vehículo, dirección.

La actividad de tratamiento a la que corresponde es: "*Registro General",* cuya finalidad es el Registro de la Entrada y Salida de documentos y remisión al departamento municipal competente, así como "*Consultas e Información sobre documentos, procedimientos, trámites o notificaciones y comunicaciones del Ayuntamiento".* Aporta detalle del registro de tratamiento. Los elementos que se tratan son necesarios por la Jefatura Provincial de Tráfico que recibe los datos y determinó el formato, orden y contenido de las celdas de la hoja.

g) Si realizaron una valoración documentada de la afectación a la confidencialidad de las personas del listado y sus derechos y que medidas de seguridad técnicas y organizativas sobre esos datos se aplicaban.

Reitera que "*La información que pudiera haber sido accedida por terceros podría ocasionar un daño a los afectados, pero inicialmente no se observa perjuicio grave*."

En cuanto a las medidas que tienen, en materia de gestión publicación de contenidos:

- Aplicación de gestión administrada según perfiles y departamentos.

- Los contendidos a publicar se realizan en soporte PDF, y conforme a la "instrucción corporativa de publicación" y "manuales de soporte" desarrollados por tipo de información o servicio.

Aporta impresión de pantalla de "*detalle la instrucción de publicación complementaria a todos los manuales corporativos*", "*nota para la publicación de contenidos desde el Gestor corporativo*".

h) Documentos generados y guardados sobre la corrección e incidencia llevada a cabo el (…) relacionado con protección de datos, tiempo que estuvo publicada la hoja, si es posible conocer cuantas visualizaciones del archivo o cuantas veces se accedió al archivo.

Aporta los documentos de entrada, la certificación interna de retirada de contenido, y el informe de 24/01/2022 REF ***REFERENCIA.1, así como el correo de comunicación a todas las unidades informando sobre el detalle de la nueva instrucción de publicación de contenidos en web y sede municipal.

Manifiesta que el documento objeto de la denuncia se publica el (…), se produce una primera desvinculación en esa misma ficha, con eliminación de 24/01/2022, sin que se disponga de números de visualizaciones o accesos al archivo.

i) Aporten la que denominan: "*la instrucción corporativa de publicación"* vigente en el momento de los hechos y sus actualizaciones y expliquen ¿por qué si en el protocolo que tenían para la gestión de la publicación de contenidos se había de realizar en pdf, la aplicación admitió anexar un tipo Excel?

Indica que en formato Excel no es utilizado para publicaciones en sede, web, si bien la aplicación si soporta ese formato, sin que sea posible restringir para adaptarlo solo a admisión de pdf. "*Actualmente se hace uso de una herramienta con mas de diez años de antigüedad*", añadiendo que en septiembre se va a actualizar la sede con el uso de un gestor de contenidos mas actual y mejoras en seguridad de publicación de contenidos.

Aporta impresión en la hoja como "*detalle instrucción complementaria a los manuales corporativos*" que contiene las notas para la publicación de contenidos en el gestor administrativo

Aporta como anexos 1 a 3, manuales de uso y "*nota para la publicación de contenidos desde el gestor corporativo*".

j) En su escrito indicó que la "*publicación de contenidos se encuentra descentralizada*", precise si no hay una unidad que centralice las instrucciones de la publicación-exposición para las cuestiones de qué datos se exponen, que tipos de documentos de cada departamento se pueden o se han de publicar, ¿cuales son de publicación obligatoria?

Manifiesta que "*actualmente no existe una unidad que centralice las instrucciones de la publicación / exposición para las cuestiones de qué datos se exponen. La instrucción operativa desarrollada con posterioridad al incidente se realizó por parte de Protección de Datos. Indicar, que existe una estrategia municipal de Gobernanza del dato e impulso del dato único, donde una de las cuestiones que se plantea es la creación de una Unidad de Organización y Gestión del Dato*".

k) En su respuesta indican que el actual DPD tomó posesión el 1/10/2021, informen si en el momento de acontecer los hechos, (…), no existía DPD y que papel asumió en la reclamación.

Manifiesta que esa labor era asumida por el Comité de Seguridad de la información, que no intervino, dado que la tramitación del incidente se realizó conforme al procedimiento de gestión de sugerencias y quejas.

l) Documentación sobre el análisis de que la brecha sea probable que constituya un riesgo para los derechos y libertades de las personas al conocerse en conjunto el NIF o NIE, nombre y apellidos, dirección y matrícula del vehículo.

Los datos estuvieron publicados y vinculados en sede, un día, "*el resto del tiempo permaneció como un documento difícil de localizar y consultar*", "*así como dado el volumen de afectados valoró de forma inicial que la información que pudiera haber sido accedida por terceros, a pesar de poder ocasionar un daño a los afectados, no observaba un perjuicio grave*".

Acompaña anexo 1, curso actas y plenos y Junta de Gobierno en la sede electrónica a través del "*Gestor de contenidos administrativos web*", anexo dos, "*curso tablón de anuncios de la sede electrónica*", en anexo tres, "*notas para la publicación de contenidos desde el gestor corporativo".*

OCTAVO: Con fecha 28/10/2022, se emitió propuesta de resolución del literal:

"*Que por la Directora de la Agencia Española de Protección de Datos se sancione con apercibimiento a* **AYUNTAMIENTO DE GETAFE***, con NIF* ***P2806500A****, por las siguientes infracciones del RGPD:*

- *Artículo 5.1.f) del RGPD.*
- *Artículo 32 del RGPD.*
- *Artículo 33 del RGPD*."

NOVENO: Con fecha 17/11/2022, se reciben alegaciones del reclamado, solicitando el archivo de actuaciones, manifestando:

1) Los datos contenidos en los archivos responden a un Convenio de Colaboración entre la FEMP y la DGT para la modificación de los permisos de conducir y de circulación de vehículos, por cambio de domicilillo, que pretende facilitar ese trámite a los ciudadanos, como se indica en la propia página web que reseña de la DGT y de la FEMP. En dicha web de la DGT se informa que el Convenio permite efectuar dichos cambios directamente en las oficinas de los Ayuntamientos suscritos al Convenio Añade el reclamado que la estructura del documento se utiliza por numerosos Ayuntamientos.

2) El documento indebido estuvo solo unas horas, se sustituyó por el correcto el mismo (…). La URL que el reclamante poseía de su acceso inicial y desde la que si era posible el acceso se proporcionó a la AEPD, era el único medio de acceso a su contenido, por lo que desde el primer momento, por medios técnicos normales no era accesible el documento, salvo que se dispusiera de la concreta URL. La confidencialidad de los datos publicados que pudo resultar afectada fue mínima, considerando que "*cabe pensar que el reclamante fue el único que accedió a los datos del listado que aportó*", y así se recoge

en la propuesta: "*el reclamante al menos pudo acceder a los datos del listado que aportó*".

El acuerdo de inicio de 4/04/2022, lo fue por la persistencia de la brecha según se indica en la propuesta, cuando lo cierto y así se da en hechos probados, es que señala, de acuerdo con el escrito de 25/01/2022 del reclamado, se contenía un informe detallado con las actuaciones realizadas, que incluían la eliminación del gestor de contenidos interno de la sede electrónica del fichero Excel, explicando la causa que motivó la errónea publicación, y las mejoras en los procedimientos. Considera por ello que falta motivación en la apertura del procedimiento.

3) No consta que la AEPD manifieste que el reclamante es un afectado por el tratamiento ni que haya sido parte en el proceso. Aún así, la Agencia continuó tramitando su denuncia pese a que los hechos se resolvieron y de que carece de pruebas sobre la afección real a los derechos de las personas afectadas. El reclamante no es interesado, los datos tratados no le conciernen, iniciándose el expediente por denuncia de un tercero ajeno, inicio de un procedimiento no previsto en el RGPD.

4) "N*o compartimos la apreciación de la AEPD sobre la infracción por falta de comunicación de la brecha de seguridad basada en el tratamiento de datos excesivo en el marco de un Convenio con la DGT, sin prueba que evidencie que los datos tratados son excesivos con respecto a su finalidad*".

5) En el fundamento de derecho sobre la infracción por falta de comunicación de la brecha de seguridad a la autoridad, art 33 del RGPD, indicando que puede "*afectar a derechos y libertades, lo que aconseja que con independencia de que se hayan producido perjuicios a los afectados y del tipo que este sea, la autoridad sea notificada.",* es calificada por el reclamado de:

-conjetura, al no aportar al AEPD prueba de lo que podría haberse producido en caso de que alguna persona hubiese accedido a los datos, y según los hechos probados, solo accedió una persona. La brecha no entraña un riesgo, dado que se consideró que no era probable que se produjeran daños y perjuicios.

-No se aporta prueba sobre lo que podría haberse producido en caso de que alguna persona hubiese accedido a los datos. No se prueban los hechos constitutivos de la infracción ni se respeta la presunción de no existencia de responsabilidad.

-En relación con la infracción imputada del artículo 32 del RGPD, se contaban con medidas organizativas para mitigar los riesgos en el tratamiento. La publicación responde a un riesgo residual producido por un error humano. "*Siempre existirá un riesgo inherente o inicial e implícito en cualquier tratamiento y, una vez que se hayan aplicado medidas y garantías que lo minimicen, seguirá existiendo un riesgo residual*". Alude a la sentencia del Tribunal Supremo, núm. 188/2022 sala tercera , sala de lo contencioso administrativo de 15/02, y expone las tesis de las obligaciones de resultados y de medios que recoge la sentencia.

HECHOS PROBADOS

1) El reclamante. al acceder en la sede electrónica del reclamado para ver una convocatoria de un Pleno, accede al documento *"*****DOCUMENTO.1** Resolución de convocatoria de sesión extraordinaria del Ayuntamiento Pleno a celebrar el ***FECHA.1"*, conteniéndose un listado de datos personales en formato excel (dirección electrónica https://sede.getafe.es/portalGetafe/sede/RecursosWeb/***(...)***). Una vez abierto, contiene datos personales de nombre, apellidos, dirección, fecha de nacimiento, número de identificación fiscal, NIE, matrícula del vehículo, y fecha de matriculación.

El reclamante pone los hechos en conocimiento del reclamado a través de una queja presentada al (…), 13 h 44 y en la misma fecha presenta reclamación ante la AEPD.

2) De acuerdo con el reclamado, la publicación concreta del contenido de la Convocatoria Extraordinaria de la Sesión Plenaria de fecha ***FECHA.1, se realizó el (…) desde su ***DEPARTAMENTO.2, que se encarga de la publicación de estos contenidos en el "*Tablón de Anuncios*" municipal en sede electrónica. El contenido objeto de la reclamación se podía ver tanto en consulta de "*actas de plenos*", como en el "*tablón de anuncios*".

3) De acuerdo con lo manifestado por el reclamado, el documento objeto de la reclamación al que se pudo acceder por el reclamante, en la sede electrónica, se expuso el mismo día que el reclamante accede, el (…) en dos sitios distintos de la sede electrónica, en "*consulta de actas de plenos*", y en "*tablón de anuncios*". El reclamado, al recibir la reclamación el mismo (…), procedió a la subsanación sustituyéndolo por el documento pdf correspondiente. ***DEPARTAMENTO.1 comprobó la corrección solo desde *opciones de navegación del portal*

***DEPARTAMENTO.1 tramitó la respuesta a la reclamación del reclamante e instó del ***DEPARTAMENTO.2, su corrección. ***DEPARTAMENTO.1 comprobó que se había corregido y se había expuesto el documento correcto, el mismo día (…), sin verificar el efectivo borrado de la URL a través del navegador.

4) El día 1/12/2021, se accedió por el inspector de la AEPD en fase de actuaciones previas al apartado correspondiente a la "*Consulta de Actas de Plenos*" de la sede electrónica del reclamado. Dentro del listado de sesiones, se consulta la correspondiente al día ***FECHA.1. El resultado de esta prueba, incorporada al expediente a través de la "*Diligencia Referencias*" no redirecciona al listado referido por el reclamante, sino a la efectiva convocatoria del citado Pleno.

A continuación, el mismo día 1/12/2021, se accede directamente a través del navegador a la dirección electrónica facilitada por el reclamante https://***sede.getafe.es/portalGetafe/sede/RecursosWeb/(...)***. El resultado de esta prueba, incorporada al expediente a través de la "*Diligencia Referencias*", es el acceso a un documento en formato Excel que contiene una hoja titulada "*SolicitudConvenioFEMP*". Los datos personales que componen dicho listado son: nombre, apellidos, dirección, fecha de nacimiento, número de identificación fiscal, matrícula del vehículo, y fecha de matriculación y coincide con el aportado por el reclamante en su reclamación.

Explica que lo sucedido respecto a aparecer el listado en el navegador, se debió a que se dejó el documento en el gestor de contenidos con el que desarrolla esta función, se desvinculó del vínculo al que se encontraba ligado inicialmente, pero no se borró el recurso, siendo posible el acceso de la ruta desde la URL y por eso aparecía en internet.

5) Manifestó el reclamado que la publicación de contenidos, en este caso la convocatoria de un Pleno, se realiza por dos unidades, ***DEPARTAMENTO.1 que publica en la sede las actas de Plenos, y ***DEPARTAMENTO.2 que publica también en la sede, en el tablón de anuncios. (…), indicando que todas las personas han recibido formación sobre protección de datos, existiendo unas instrucciones escritas que se dan en cursos para la gestión de la publicación de recursos de contenidos.

6) El documento objeto de la reclamación al que el Inspector de la AEPD pudo acceder el 1/12/2021 a través del navegador, fue borrado del mismo con fecha 24/01/2022, no siendo ya accesible en internet.

Mediante la corrección de la URL en el navegador, se aprobó una instrucción que mejora de forma operativa las garantías en fase de publicación de contenidos de datos personales. Esta instrucción es aplicable tanto en la publicación de contenidos de web municipal como en los de la sede.

7) El documento al que pudo acceder el reclamante es un documento de trabajo que se remite cada semana por el reclamado a la Jefatura Provincial de Tráfico como resultas de un Convenio con la Federación Española de Municipios y Provincias, para facilitar a los ciudadanos que el trámite de cambio de domicilio pueda realizarlo en la oficina municipal. El documento es tramitado por el ***DEPARTAMENTO.2 del reclamado, misma entidad que lo expuso originariamente en la sede electrónica cuando el reclamante accedió.

8) El registro de tratamiento que se aplica a los datos objeto de la reclamación es el de "*Registro General*".

9) El reclamado disponía para la gestión de publicación de contenidos:

- Los contendidos a publicar se realizan en soporte PDF, y conforme a la instrucción corporativa de publicación y manuales de soporte desarrollados, por tipo de información o servicio, si bien el que se subió era Excel.

- Aplicación de gestión, administrada según perfiles y departamentos, en este caso, la convocatoria del Pleno la publica el ***DEPARTAMENTO.2, uno de los dos Departamentos habilitados.

Aporta impresión de pantalla de "*detalle la instrucción de publicación complementaria a todos los manuales corporativos*", "*nota para la publicación de contenidos desde el Gestor corporativo*".

10) Como acciones tomadas a consecuencia de la reclamación, se ha añadido una nota a las instrucciones para la publicación de contenidos, para que se tenga en cuenta en el gestor de contenidos corporativo en la que participó "Protección de Datos", se efectuó una formación del caso y se ha instado una revisión cruzada de lo que se publica en la sede o en la web, "*por parte de otra persona del mismo departamento*".

11) El reclamado no estimó oportuno notificar a los afectados porque el mismo día de su publicación eliminó el contenido de la sede y sobre la permanencia en el navegador, manifiesta que la búsqueda precisaba de introducir la especifica URL, cuando ya (…) no figuraba en la sede porque fue eliminada, acreditándose no obstante la certeza de poder haber accedido mientras ha permanecido, es decir, hasta el 24/01/2022.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*."

II

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que el reclamado realiza la recogida, registro, acceso, utilización de datos personales de personas físicas, tales como: nombre, número de identificación, etc. como se acredita del fichero Excel al que tuvo acceso el reclamante.

El reclamado realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "*violaciones de seguridad de los datos personales" (en adelante brecha de seguridad) como "todas aquellas violaciones de la seguridad que ocasionen 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*."

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad; consecuencia de la exposición en sede electrónica de un archivo indexado que no se correspondía con el pretendido, y que contenía datos personales. El proceso para llevarlo a efecto es un proceso de intervención humana que contaba con un protocolo propio y se desarrollaba con un gestor de contenidos corporativo como herramienta para llevarlo a efecto.

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Los artículos 32, 33 y 34 del RGPD, regulan la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III

Artículo 5.1.f) del RGPD

Se imputa al reclamado una infracción del artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD que establece:

"*1. Los datos personales serán:*
(…)

f) 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 («integridad y confidencialidad»)."

En el presente caso, queda acreditado que se ha producido un acceso no autorizado a los datos personales de los integrantes del archivo tipo Excel que el reclamante puso en su sede electrónica, al que tuvo acceso el reclamante y que se mantuvo en el navegador, vulnerándose el principio de confidencialidad. La AEPD verifica que al menos, a 1/12/2021, es todavía posible el acceso al contenido tecleando la dirección electrónica en el navegador.

De conformidad con las evidencias de las que se dispone, se considera que los hechos conocidos son constitutivos de una infracción, imputable al reclamado, por vulneración del artículo 5.1.f) del RGPD.

El reclamante al menos pudo acceder a los datos del listado que aportó. El mismo listado figuró hasta 24/01/2022 en el navegador, acreditándose la citada infracción.

IV

Tipificación de la infracción del artículo 5.1.f) del RGPD

La infracción del artículo 5.1.f) del RGPD supone la comisión de la infraccione tipificada en el artículo 83.5 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*", establece que "*Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica*".

A efectos del plazo de prescripción, el artículo 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:

"1*. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"

V

Sanción por la infracción del artículo 5.1.f) del RGPD

El Artículo 83 "*Condiciones generales para la imposición de multas administrativas*" del RGPD apartado 7 establece:

"Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro."

Asimismo, el artículo 77 "*Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento" de la LOPDGDD dispone lo siguiente:*

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:…

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local…

2. 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 sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.
(…)

5. Se 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. (…)"

Por tanto, la citada infracción del artículo 5.1.f) del RGPD, correspondería sancionar con apercibimiento al reclamado.

VI

Artículo 32 del RGPD

El Artículo 32 del RGPD establece:

"Seguridad del tratamiento

1. 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.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

El considerando 75 del RGPD enumera una serie de factores o supuestos asociados a riesgos para las garantías de los derechos y libertades de los interesados: "*Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o*

cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados."

Cada tratamiento debe estar sujeto a un conjunto de medidas de seguridad según la probabilidad y el riesgo para los derechos y libertades de las personas físicas, que debe determinarse con referencia a la naturaleza cómo era el cáncer como el contexto y los fines del tratamiento de datos y dicho riesgo debe ponderarse sobre la base de una evaluación objetiva

El considerando 83 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*" "*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*". El riesgo se relaciona así, con las medidas que han de ser tomadas, que además han de ser adecuadas

Las que se citan en el artículo 32 del RGPD, son un conjunto no exhaustivo de las que se pueden tomar.

En este caso, lo que se pretendía publicar era una convocatoria de Pleno, que en principio trataría de los puntos de discusión del orden del día. En su lugar se introdujo otro archivo y en otro formato del que surgen las tres conductas infractoras.

Se parte de la publicación del archivo en la sede, para que el público pudiera acceder, y descargar el archivo debiendo tener en cuenta el tipo de contenido, el formato y la previsualización antes de su efectiva publicación, dados los riesgos que presenta dicho tipo de tratamiento, que prevenga o ayude a que no se presenten los riesgos.

El reclamado debe contar con un sólido y completo protocolo que debe no solo prevenir que se produzca la contingencia, sino, una vez acontecida esta en su caso, como correctiva, reaccionar ante la materialización del riesgo, que al aplicarse, pueda garantizar la seguridad en el tratamiento de la información y de los datos.

La toma de medidas ha de comprender el impacto que para los derechos y libertades podría tener un incidente, se produzca de modo accidental, humano, natural o tecnológico y dirigirse tanto a reducir el impacto como su probabilidad, las cuales deben estar en constante renovación y mejora

En este caso, cuando se produjo la inicial corrección (…), no se tuvo en cuenta que el documento, por la forma y el medio de implementarse, quedó vigente en gestor de contenidos, pudiéndose visualizar en el navegador, sin que técnicamente se hubiera tenido en cuenta la operativa de la aplicación que genera los contenidos, ni haberse contado con la participación en el proceso de personal técnico especializado como el de informática que parece evidente, si conoce los efectos de publicación en sede electrónica y en navegador.

Los fallos de las medidas de seguridad que puedan cometer los empleados en una entidad jurídica, no se imputarán a esta siempre que hubiese adoptado todas las medidas de prevención posibles, y en este caso, se considera que esta verificación como medida técnica, en relación a la naturaleza del tratamiento, la tecnología empleada: exposición en sede electrónica con un programa informático de gestor de contenidos además de necesitar una pronta respuesta en caso de quiebra, exige estos elementos como razonablemente exigibles, elementos que no tuvieron lugar en su momento. al no atajar del todo la brecha producida, porque no estaban establecidas cuando se produjeron los incidentes. El reclamado debía haber evaluado correctamente los riesgos de la falta de confidencialidad en sus protocolos de identificación de riesgos adicionales generados por la brecha incluyendo los correspondientes a las acciones humanas. Además, la tecnología adoptada en el tratamiento de publicación con una herramienta de gestión de contenidos que como soporte no estuvo presente en el citado protocolo, teniendo que añadirlo cuando se descubrió a que obedeció el fallo. Por tanto, se acredita la falta de una correcta consideración de atención las medidas organizativas y técnicas en la configuración de las medidas de seguridad infringidas en el presente supuesto.

- A ello se debe añadir que la reclamación se traslada al reclamado el ***FECHA.2, recibida_el 4/05/2021, haciéndole saber los hechos, sin obtenerse respuesta, dejando transcurrir el tiempo sin atender la petición. Se dirigió ya por la AEPD escrito al reclamado en fase de actuaciones previas el 10/09/2021 en modalidad de notificación electrónica y teniendo que reiterar por vía postal, al rechazar la primera, recibiendo esta ultima el ***FECHA.4 sin obtener atención a lo solicitado, para, finalmente, el 25/01/2022 recibirse escrito del reclamado, en el que entre otros extremos explica que "*el retraso en la respuesta se debió a que en dicho periodo hubo una transición de responsabilidades en materia de protección de datos entre el Comité de Seguridad de la Información, órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información, y la Delegada de Protección de Datos cuya toma de posesión tuvo lugar el 1/10/2021*".

- Cuando se recibe escrito de 25/01/2022 del reclamado, lo primero que indica es que responde a la petición de información cursada, recibida el ***FECHA.4, y no se conocía aun la pervivencia de la información en el navegador, que se diligencia el 1/12/2021.

En la petición de información se pone en conocimiento la URL en la sede electrónica así como la dirección https.

Además, se solicitaron hasta doce cuestiones de información, que se respondieron secuencialmente, y en las acciones tomadas, no se alude a la corrección de 24/01/2022 de modo expreso, En la respuesta que da en el punto 9 sobre la violación de seguridad y notificación, tampoco señala aspecto alguno, extendiendo la toma de posesión del DPD relacionada con la falta de notificación a la autoridad de control

En cuanto a la aclaración de la subsanación de la pervivencia de la posibilidad de acceso, solo se indicó que "*A fecha de hoy 24/01/2021, desde el Departamento de informatica se ha procedido a revisar todo el contenido informativo almacenado y publicado tanto en la web como en la sede municipal, no habiéndose encontrado ningún recurso en soporte similar ni en cuyo contenido haya datos de carácter personal*".

La retirada de la URL del gestor de contenidos es conocida plenamente en el período de pruebas cuando expresamente se solicita en una de ellas y se responde especificando que se ha eliminado del gestor de contenidos con intervención de la unidad de informática el 24/01/2022.

También quedó aclarada la finalidad y objeto del listado de datos que antes de dicha prueba no se explicó.

Así pues, no resulta cierto que se conocieran los detalles de la infracción cuando se acuerda el inicio del procedimiento.

Además, que el reclamante sea interesado o no en el procedimiento, que sus datos sean afectados o no, no incide en la validez de dicho acuerdo, dado que el procedimiento se inicia siempre de oficio. (art 58 de la LPCAP). Tampoco la manifestación de que no hay pruebas sobre la afección real a derechos implicaría que la autoridad de control pueda solicitar y contrastar el cumplimiento de las obligaciones impuestas por el RGPD, obtener una explicación de lo sucedido, y analizar las medidas existentes y las derivadas. El hecho de que no se acredite afección real a terceros no quiere decir que no la haya habido o podía haberla habido, acreditándose que los datos se han puesto en evidente riesgo al transcurrir varios meses con la posibilidad de que en el navegador se obtuvieran los resultados, bien accediendo directamente a su literal, bien por otros medios.

Se acredita que el reclamado ha infringido el citado artículo.

VII

Tipificación de la infracción del artículo 32 del RGPD

De confirmarse, la citada infracción del artículo 32 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica "*Condiciones generales para la imposición de multas administrativas*" dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)

"f) 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.

(…)

VIII

Sanción por la infracción del artículo 32 del RGPD

De conformidad con la aplicación de los artículos 83.7 del RGPD y 77.1.c) de la LPDGDD, como se explicó en el fundamento de derecho V para la infracción del artículo 5.1.f) del RGPD, correspondería sancionar con apercibimiento al reclamado por la infracción del artículo 32 del RGPD.

IX

Artículo 33 del RGPD

El artículo 33 "*Notificación de una violación de la seguridad de los datos personales a la autoridad de control*" del RGPD, establece:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
…

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;

b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;

c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;

d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

En el presente caso, consta que el reclamado ha sufrido una brecha de seguridad de los datos personales en fecha 31/03/2021 y no ha informado a esta Agencia.

Una violación de la normativa de datos puede tener una serie de efectos adversos considerables en las personas, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales. En el RGPD se explica que estos efectos pueden incluir la pérdida de control sobre sus datos personales, la restricción de sus derechos, la discriminación, la usurpación de identidad o fraude, las pérdidas financieras, la reversión no autorizada de la seudonimización, el daño para la reputación y la pérdida de confidencialidad de datos personales sujetos al secreto profesional. También puede incluir cualquier otro perjuicio económico o social significativo para esas personas.

Conforme al principio de responsabilidad proactiva, no sería obligatorio notificar todas las brechas, dado que el responsable podría garantizar que es improbable que la brecha de datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El reclamado ha definido la relación que tiene el colectivo titular de los datos con el Ayuntamiento, que era la de facilitar la modificación de los permisos de conducir y circulación de vehículos por cambio de domicilio que se podía efectuar mas cómodamente en la oficina del Ayuntamiento. Sin embargo frente a esta facilitación de los

tramites, desde (…) hasta 24/01/2022, ha existido un riesgo posible y cierto de que en internet, no en la sede, se pudiera acceder a una serie de datos que configuran la identidad de las personas con la reunión simultanea de varios datos que añaden información sobre las mismas, que sí que es probable que constituya un riesgo para los derechos y las libertades de esas personas.

Cuando sucede una brecha de datos personales es necesario que el responsable determine de forma rigurosa cuáles son las posibles consecuencias, cómo pueden afectar a los derechos y libertades de las personas afectadas, es decir el nivel de severidad con el que se podrían materializar dichas consecuencias y la probabilidad de que se materialicen. La alegación hecha para no tener que notificar la brecha de que la *"información que pudiera haber sido accedida por terceros podría ocasionar un daño a los afectados, pero inicialmente no se observa un perjuicio grave*" no sirve de excusa para que considerándose ciertamente que con independencia de conocer cuantas personas han podido acceder durante el tiempo que estuvo expuesta la información, sí que apunta a la existencia cierta de riesgos para los derechos y libertades de los diecisiete afectados por la infracción, dado el contenido conjunto de los diversos datos que se dan a conocer, y su relevancia en afectación de derechos y libertades, que con independencia de que se hayan producido perjuicios a los afectados, a lo que no se refiere el tipo, se obliga a que la autoridad sea notificada.

Se considera que los hechos infringen el artículo 33 del RGPD.

X

Tipificación de la infracción del artículo 33 del RGPD

Supone la infracción del artículo 33 del RGPD la comisión de una infracción tipificada en el artículo 83.4 del RGPD que dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"

A este respecto, la LOPDGDD, en su artículo 71, indica: "*Infracciones*" establece que *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".*

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD, indica:

"En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una

vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

(…)

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679. (…)"

XI

Sanción por la infracción del artículo 33 del RGPD

De conformidad con la aplicación de los artículos 83.7 del RGPD y 77.1.c) de la LPDGDD, como se explicó en el fundamento de derecho V para la infracción del artículo 5.1.f) del RGPD, correspondería sancionar con apercibimiento al reclamado por la infracción del artículo 33 del RGPD.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: SANCIONAR a **AYUNTAMIENTO DE GETAFE**, con NIF ***P2806500A***, con un apercibimiento por cada una de las siguientes infracciones:

-Del artículo 5.1.f) del RGPD, de conformidad con el artículo 83.5.a) del RGPD, y a efectos de prescripción, tipificada como muy grave, según el artículo 72.1 a) de la LOPDGDD.

-Del artículo 32 del RGPD, de conformidad con el artículo 83.4.a) del RGPD, y a efectos de prescripción, tipificada como grave, según el artículo 73. f) de la LOPDGDD.

- Del artículo 33 del RGPD, de conformidad con el artículo 83.4.a) del RGPD, y a efectos de prescripción, tipificada como grave en el artículo 73.r) de la LOPDGDD

SEGUNDO: NOTIFICAR la presente resolución a **AYUNTAMIENTO DE GETAFE**.

TERCERO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

CUARTO: De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5

de la disposición adicional cuarta de la Ley 29/1998, de 13/07, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1/10. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-181022

Mar España Martí
Directora de la Agencia Española de Protección de Datos