- **Expediente Nº: EXP202201318**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 23 de marzo de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***BARNA PORTERS SEGURETAT, S.L.*** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202201318

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO***: D. A.A.A.*** (en adelante, la parte reclamante), en fecha 27 de diciembre de 2021, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra BARNA PORTERS SEGURETAT, S.L. con NIF B62735089 (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

En el escrito recibido en esta Agencia se reporta una vulnerabilidad en la página web de la compañía BARNA PORTERS SEGURETAT, S.L., existente desde hace un año.

Según se explica, al pinchar con el ratón en un icono con forma de lupa roja que aparece en la esquina superior izquierda de la pantalla correspondiente a la sección "Accés Serviap", (cuyo enlace se encuentra en el pie de la mencionada página web), se descarga automáticamente en el equipo, un fichero Excel de autorizaciones de Covid-19, con (…) entradas, que contiene la siguiente información: (…).

Los servicios de Inspección de esta Agencia han constatado que, en el momento de presentación de la reclamación, la vulnerabilidad seguía existiendo.

Junto a la reclamación aporta Fichero Excel completo que contiene autorizaciones de Covid-19, con (...) entradas y juego de imágenes para explicar cómo se accede a dicha información.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, fue recibido en fecha 11 de febrero de 2022, como consta en el certificado que obra en el expediente.

En fecha 11 y 16 de marzo de 2022, se recibe en esta Agencia escrito de respuesta indicando que la notificación remitida por la Agencia es la primera comunicación recibida por la que tienen conocimiento de la vulneración comunicada, no habiendo recibido comunicación previa del denunciante ni de ningún otro posible afectado.

Manifiesta que SERVIAP, como intranet o herramienta interna de la empresa, es una herramienta privada, desarrollada a medida por ENDURO WEB TOURS SL con CIF B66390725 (encargado del tratamiento), en adelante ENDURO, a la que sólo tienen acceso usuarios autorizados (mediante usuario y contraseña), por lo que no es accesible a personas sin vínculo con la empresa.

Nadie sin relación o ajeno a la empresa, puede tener acceso a estos datos personales, a excepción, obviamente, del incidente comunicado, provocado por un error de programación durante el desarrollo de unas pruebas de la nueva versión de la intranet corporativa. Señala que hasta la fecha no se ha recibido queja alguna por parte de ninguna persona acerca de dicha circunstancia.

Explica que la causa que ha ocasionado la reclamación ha sido un fallo de programación:

- Su proveedor informático, ENDURO es el mismo que desarrolla la aplicación SERVIAP como herramienta interna de intranet de la empresa, a la que tienen acceso los trabajadores. Dicha aplicación se ha desarrollado a medida.

- En su momento, cumpliendo con la obligación de facilitar a los trabajadores un “certificado de autorresponsabilidad Covid-19”, se programó un formulario autorrellenable de autorización de movimiento del personal en horario de restricción COVID-19.

Dicho formulario, sólo era accesible para los usuarios registrados, trabajadores de la empresa, no conteniendo datos personales, hasta que fuese rellenado por los propios trabajadores, por lo que los datos que constan introducidos han sido facilitados por los propios usuarios.

Los datos personales, consistentes en (…) quedaban guardados en una base de datos.

Es esta base de datos, la que alimentó el fichero al que se accedía de forma accidental en el icono logo de Serviap que consta en la parte superior izquierda de la página de acceso https://serviap.cat/ durante unas pruebas de una nueva versión de Serviap.

- Dado que se estaba trabajando en una versión más avanzada y con mayores funcionalidades de Serviap para sustituir la versión v19.51, a finales de 2021, se realizaron unas pruebas de programación, alimentando con aquella base de datos el listado al que podía accederse de forma accidental tal y como se ha señalado con anterioridad.

El icono “con forma de lupa roja” que consta en la parte superior izquierda de la página de acceso a SERVIAP, donde fue detectada la vulnerabilidad, no se trata de ninguna herramienta de búsqueda, sino que dicho icono corresponde al logo de la aplicación, por lo que no es operativo ni contiene acceso para los usuarios.
Expone que la vulnerabilidad ha sido causada por un error de programación de uno de los técnicos informáticos (programador junior) que insertó accidentalmente un enlace que permitía la descarga del fichero.

El listado, que ha dado motivo a la denuncia formulada, ha sido eliminado del enlace accidental, una vez se ha tenido conocimiento de dicha circunstancia, esto es a la recepción del requerimiento formulado por la Agencia, en fecha 11 de febrero de los corrientes.

Dicho icono (el logo de la aplicación), nunca ha sido diseñado ni señalado como un acceso a la herramienta, no siendo tampoco objeto de acceso a una base de datos pública ni de información con la excepción de ser únicamente el logo identificativo de la intranet corporativa.

Indica que una vez comunicada la vulnerabilidad y verificada ésta, ENDURO revisó la página de inicio de la intranet y procedió de manera inmediata a eliminar el enlace que daba acceso de manera accidental al listado, por lo que dicha vulnerabilidad fue eliminada.

Tanto desde la organización como el delegado de protección de datos de esta pudieron comprobar que dicha vulnerabilidad fue anulada y que ya no era posible acceder al fichero esa misma tarde.

En cuanto a las medidas adoptadas por el responsable para solucionar la citada situación han sido:

a) Contactar con el proveedor encargado de la programación y mantenimiento de la intranet corporativa para que eliminase de forma inmediata, el enlace accidental en el icono (logo de la intranet) que consta en la parte superior izquierda de la página de acceso a Serviap.
b) Registrar la vulneración comunicada en el Registro de Incidencias.
c) Depurar el fichero excel para conocer el número y las personas afectadas.

d) Informar a los usuarios mediante aviso en la propia intranet.

En cuanto a las medidas adoptadas para evitar que se repita dicha situación han sido:

a) Reiterar al encargado del tratamiento las obligaciones en materia de protección de datos.
b) Solicitar el traslado de la dirección y supervisión de la programación, mantenimiento y pruebas de la intranet Serviap a un programador senior con más años de experiencia. A este respecto, cabe señalar el compromiso por parte de Enduro, que se ha comprometido a encargar dichas labores a un programador senior con más de años de experiencia.

Se indica a su vez que debe evitar realizar pruebas con datos reales.

Los datos afectados por la vulneración detectada consisten en: (…).
Indica que el fichero accesible a través de la vulnerabilidad comunicada contenía (…) entradas, muchas de ellas repetidas y que, una vez depuradas las repeticiones, y restada la línea de encabezamiento, el usuario “Demo” y el usuario “No Vale” se constata un total de (…) personas afectadas sin que entre las mismas haya ningún menor.

Dado que el acceso a la página de la intranet de la empresa https://serviap.cat/ se realiza mayoritariamente, por no decir en exclusiva, por el personal de la organización, se estima baja la incidencia o posibles consecuencias para las personas afectadas.

En cuanto a la comunicación del incidente a la AEPD, manifiesta que, dado que el responsable ha tenido conocimiento de dicha vulneración a través de la notificación remitida por la propia Agencia Española de Protección de Datos, la organización no ha considerado necesario notificar la brecha a la AEPD conforme al art. 33 RGPD, al tener ya conocimiento de esta, puesto que fue la propia autoridad quien comunicó a la organización la vulnerabilidad detectada.

Por último, indica que la organización se encuentra firmemente comprometida con el cumplimiento normativo no sólo en las áreas donde presta sus servicios: vigilancia de instalaciones y protección de bienes, establecimientos, espectáculos, certámenes o convenciones, custodia de llaves y acudas, explotación de central receptora de alarmas, protección de personas e instalaciones y mantenimiento de aparatos y dispositivos de seguridad; sino con la mejora continua y estándares de calidad.

En relación con las afirmaciones anteriores, la parte reclamada proporciona la siguiente documentación:

- Documento número UNO detalle del tratamiento “Laboral y RRHH”, donde se puede apreciar, entre otros:
  - estructura del fichero,
  - principios del tratamiento,
  - política de seguridad, y
  - medidas de protección de datos.
- Documento número DOS: fichero Excel depurado, conteniendo el listado de las personas afectadas y ordenado alfabéticamente.

- Documento número TRES: Informe emitido por el Delegado de Protección de Datos acerca del incidente.
- Documento número CUATRO: Certificado ISO 27001
- Documento número CINCO: Informe final Auditoria 2021, ISO 27001 donde se puede apreciar que en fecha 15.05.2021 no se detectó ninguna incidencia, ni hubo hallazgo alguno que señalase la vulnerabilidad comunicada.

TERCERO: En fecha 27 de marzo de 2022, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

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 las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 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:

ENTIDADES INVESTIGADAS

BARNA PORTERS SEGURETAT, S.L. con NIF B62735089 con domicilio en ARIZALA, 43 - 08028 BARCELONA (BARCELONA)

ENDURO WEB TOURS SL con NIF B66390725 con domicilio en C/ BRUC, 3. - 08758 CERVELLÓ (BARCELONA)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Con fecha 16 de junio de 2022 se constata que el enlace a la descarga del fichero desde la página web https://serviap.cat ha desaparecido.

Con fecha 16 de junio de 2022 se verifica que realmente existe una página web https://serviap.cat/21serviap.asp en desarrollo. Se graba en el sistema SIGRID, como objeto asociado, la captura de pantalla de la página de inicio de esta web en desarrollo.

Tras la solicitud de información adicional requerida por parte de esta Agencia a BARNA PORTERS con fecha 7 de julio de 2022, la parte reclamada remite a esta Agencia, con número de registro de entrada en la AEPD REGAGE22e00032239897 y fecha 26 de julio de 2022, la siguiente documentación:

- Registro de actividades del tratamiento
- Registro de violaciones de seguridad
- Contrato de encargado de tratamiento con CLAU informática
- Contrato de encargado de tratamiento con LEITIC
- Contrato de encargado de tratamiento con ENDURO
- Formulario cumplimento encargados de tratamiento/proveedores
- Contrato de confidencialidad para proveedores
- Certificado de garantía de cumplimiento del RGPD

Se comprueba que el Registro de actividades de tratamiento proporcionado por la parte reclamada contiene toda la información que recoge al respecto el artículo 30 del RGPD.

Se analiza el Registro de violaciones de seguridad, verificando que se ha incluido la incidencia producida el 11 de febrero de 2022 junto con toda la información necesaria para tratarla:

- Tipo de incidencia
- Persona que notifica la incidencia
- Persona encargada de la resolución
- Ficheros afectados
- Descripción
- Efectos ocasionados
- Medidas correctoras

En este registro se detalla que, habiendo sido informados los trabajadores mediante aviso en la intranet corporativa, no se ha presentado reclamación alguna por parte de los afectados a fecha 10 de marzo de 2022.

Las medidas correctoras que se especifican en el registro son las siguientes:

- 13.37h Se ha comunicado incidente a DPD.
- 13.38h Se ha contactado con el encargado de datos responsable de la programación y mantenimiento de la página web. Se le informa de la vulnerabilidad notificada y se le requiere proceda a revisar y realizar las medidas correctoras oportunas para cancelar la descarga automática del archivo al pinchar sobre el icono en la esquina superior izquierda.
- 14.02h Se ha eliminado enlace accidental que permitía la descarga del fichero.
- 14.07h Se comunica a DPD la eliminación de la vulnerabilidad
- 14.16h Se contacta de nuevo con ENDURO:

a) se le han reiterado las obligaciones en materia de protección de datos como ET y se le recuerda que debe evitarse realizar pruebas con datos reales.
b) se le ha solicitado que la dirección y supervisión de la programación, mantenimiento y pruebas de la intranet Serviap se asigne a un programador senior con más años de experiencia.

Se aceptan dichas cuestiones por el proveedor.

Manifiesta en su escrito el reclamado que, tras la comunicación de la vulnerabilidad detectada por parte de la AEPD el 11 de febrero de 2022 y la resolución de esta de manera casi inmediata, se procedió a publicar el 14 de febrero de 2022 en la intranet aviso sobre la incidencia detectada.

Encargados y roles

En su escrito de respuesta, la parte reclamada continúa exponiendo los roles desempeñados por los distintos proveedores con los que mantienen contratos de encargados de tratamiento y adjuntan copia de dichos contratos.
Respecto a ENDURO, especifica que se trata de su proveedor informático: se ocupa tanto del mantenimiento de sistemas y aplicaciones, como del desarrollo de la aplicación SERVIAP como herramienta interna de intranet de la empresa, a la que tienen acceso los trabajadores
Revisado el contrato entre BARNA PORTERS, como responsable del tratamiento, y ENDURO, como Encargado del tratamiento, se observa que en dicho contrato se tienen en cuenta los aspectos especificados en el artículo 28.3 del RGPD.

. - Objeto, duración, naturaleza y la finalidad del tratamiento.
. - Tipo de datos personales y categorías de interesados.
. - Obligaciones y derechos del responsable.
. - Obligaciones y derechos del Encargado.
En este apartado se incluye la obligación de tratar los datos personales únicamente para el fin del encargo.
. - Personal autorizado para realizar el tratamiento.

En este apartado, el encargado garantiza que el personal ha recibido la formación necesaria para asegurar que no se pondrá en riesgo la protección de datos personales.
A este respecto, se verá más adelante que ENDURO ha proporcionado un certificado de formación en protección de datos para el personal de su empresa autorizado para el tratamiento de datos personales.

. - Medidas de seguridad.

En este apartado, el ENCARGADO manifiesta estar al corriente en lo que concierne a las obligaciones derivadas de la normativa de Protección de Datos, especialmente en lo que se refiere a la implantación de las medidas de seguridad para las diferentes categorías de datos y de tratamiento establecidas en el artículo 32 del RGPD.

El ENCARGADO garantiza que se implementarán adecuadamente dichas medidas de seguridad y ayudará al responsable a cumplir las obligaciones establecidas en los artículos 32 al 36 del RGPD.

. - Violación de seguridad.
. - Comunicación de datos a terceros.
. - Transferencias internacionales de datos.
. - Subcontratación del tratamiento de datos.
. - Derechos de los interesados.

En este apartado se especifica la asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados.

. - Responsabilidad
. - Fin de la prestación del servicio.

Se especifica que, a elección del responsable, el encargado deberá suprimir o devolver los datos almacenados.

Idoneidad de ENDURO como desarrollador y encargado

Consultada la parte reclamada sobre las características e idoneidad de ENDURO para realizar el desarrollo de la aplicación SERVIAP, BARNA PORTERS explica por qué considera que esta empresa ofrece garantías suficientes como encargada para aplicar medidas técnicas y organizativas apropiadas y lo justifica aportando la siguiente documentación:

. - Formulario cumplimento encargados de tratamiento/proveedores
. - Contrato de confidencialidad para proveedores
. - Certificado de garantía de cumplimiento del RGPD

Con fecha 07 de Julio de 2022 se solicita información a ENDURO.
En esa misma fecha, la notificación se pone a su disposición mediante sistema de notificaciones electrónicas Notific@, en el que consta fecha de rechazo automático: 18 de julio de 2022.
Se reitera dicha solicitud mediante los servicios postales, siendo esta notificación entregada el 02 de agosto de 2022.
Con fecha 12 de agosto de 2022 y con número de registro de entrada en la AEPD REGAGE22e00035200405, ENDURO remite a esta Agencia la siguiente información y manifestaciones:

Metodologías de desarrollo y protocolo de pruebas

Consultada sobre las metodologías de desarrollo que sigue ENDURO en un proyecto de estas características y los protocolos de desarrollo y pruebas antes de llevar una nueva versión a producción, ENDURO explica detalladamente las necesidades, requisitos, arquitecturas y funcionalidades de la aplicación, junto con el ciclo de vida (incluyendo metodología de pruebas) y el tratamiento de los datos en las distintas capas de la aplicación.

Los responsables del proyecto realizan una serie de pruebas para confirmar la viabilidad y la utilidad de la solución. Si cumple con lo establecido en la fase de diseño, se implementa en procesos que lo requieran. Si no es así, se deben tomar medidas para corregir los fallos que impidan su normal desarrollo.

Requerido el catálogo de pruebas que se han llevado a cabo antes de desplegar la nueva versión de SERVIAP en producción (es decir, en particular para este caso de desarrollo de nueva versión de SERVIAP), ENDURO no aporta evidencias particulares para este asunto.

Cualificación técnica del personal

Respecto a la cualificación técnica de las personas involucradas en el proyecto de desarrollo, ENDURO prosigue especificando los perfiles técnicos que han intervenido en cada parte del proyecto. Intervienen figuras como analista, diseñador, programador y formador.

Formación en protección de datos

En este sentido, ENDURO detalla que realiza formaciones de forma anual y proporciona un certificado de formación en protección de datos en el que se especifica, entre otros puntos, que ENDURO ha recibido información adecuada y suficiente para adaptarse y mantenerse actualizada al RGPD y para transmitirla al personal autorizado para el tratamiento de datos personales

Fichero origen de la brecha y enlace accidental

Consultada sobre la finalidad de la creación del fichero origen de la brecha, ENDURO expone que, debido a las restricciones de desplazamiento y toque de queda a causa de la epidemia COVID-19, fue necesario implementar un formulario para el personal de la empresa.
La información contenida en ese fichero facilitaba la confirmación a terceros, principalmente fuerzas y cuerpos de seguridad y excepcionalmente (por seguridad) a cliente final que el trabajador desplazado se desplazaba para cubrir un puesto/localización determinada.
ENDURO manifiesta que, durante el desarrollo de la nueva versión de la intranet corporativa, parece ser que uno de los programadores pegó accidentalmente por error el enlace de acceso interno al archivo en el logo de la página de acceso a la intranet corporativa, a finales de noviembre, principios de diciembre de 2021.

Recurrencia incidentes y vulnerabilidades

Concluye ENDURO destacando que el enlace accidental fue eliminado de manera inmediata en cuanto se tuvo conocimiento de ello y que este es el primer incidente al que se ha enfrentado dicha empresa.

CONCLUSIONES

Brecha de seguridad de confidencialidad provocada por un error de programación que permite la descarga de un fichero Excel que contiene datos personales de los trabajadores de la empresa.
El reclamado BARNA PORTERS reconoce que el enlace de acceso al archivo se pegó por error en el logo de la página de acceso a la intranet corporativa.
ENDURO sitúa el pegado del enlace a finales de noviembre, principios de diciembre de 2021.
El enlace accidental se eliminó de manera inmediata en cuanto se tuvo conocimiento de ello. La brecha se solventó el 11 de febrero de 2022.
No se ven afectadas la disponibilidad ni la integridad de los datos personales, puesto que ese enlace permitía la descarga del fichero, pero no la modificación del fichero en su servidor.
Las medidas adoptadas por el responsable para solucionar la brecha se consideran adecuadas.
La parte reclamada ha informado a los usuarios mediante un aviso en la intranet, publicado el primer día laboral posterior al conocimiento de la brecha.
La parte reclamada no notificó la brecha a la AEPD puesto que fue la propia AEPD quien comunicó a la organización la vulnerabilidad detectada.

El contrato de encargado de tratamiento entre BARNA PORTERS, como responsable del tratamiento, y ENDURO, como Encargado del tratamiento tiene en cuenta los aspectos especificados en el artículo 28.3 del RGPD.
En particular, el apartado de medidas de seguridad indica que el ENCARGADO manifiesta estar al corriente en lo que concierne a las obligaciones derivadas de la normativa de Protección de Datos, especialmente en lo que se refiere a la implantación de las medidas de seguridad.
ENDURO ha proporcionado información sobre los protocolos de pruebas que se llevan a cabo antes de llevar una nueva versión a producción, pero no ha aportado evidencias de las pruebas que se han efectuado en este caso particular.
Aunque el error de programación que ha causado la brecha de seguridad es improbable que hubiera sido detectado en una batería de pruebas (puesto que no es una funcionalidad que se estuviera implementando), ENDURO no ha proporcionado evidencias que constaten que en este caso se haya efectuado la batería de pruebas antes de llevar la versión a producción.

QUINTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad BARNA PORTERS SEGURETAT, S.L. es una gran empresa constituida en el año 2001, (…).

FUNDAMENTOS DE DERECHO

I
Competencia

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
Cuestiones previas

BARNA PORTERS SEGURETAT, S.L. es una empresa con forma jurídica de sociedad limitada dedicada a actividades de seguridad privada, para lo cual trata datos de carácter personal de sus clientes y trabajadores, entendiendo por dato de carácter personal: *"toda información sobre una persona física identificada o identificable*".

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:

«responsable del tratamiento» o «responsable»: *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros*

Se considera persona física identificable aquella 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.

Asimismo, debe entenderse por tratamiento "*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".*

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 provocada por un error de programación que permitió la descarga de un fichero Excel que contenía datos personales de los trabajadores de la empresa.

Los datos afectados por la vulneración detectada fueron: (…). No se vieron afectadas la disponibilidad ni la integridad de los datos personales, puesto que el enlace permitía la descarga del fichero, pero no la modificación del fichero en su servidor.

El fichero accesible a través de la vulnerabilidad comunicada contenía (…) entradas, muchas de ellas repetidas, si bien, una vez depuradas las repeticiones se constata un total de (…) personas afectadas sin que entre las mismas haya ningún menor.

Dado que el acceso a la página de la intranet de la empresa se realiza mayoritariamente, por no decir en exclusiva, por el personal de la organización, se estimó baja la incidencia o posibles consecuencias para las personas afectadas.

El enlace accidental se eliminó de manera inmediata en cuanto se tuvo conocimiento de ello. La brecha se solventó el 11 de febrero de 2022.

Según el GT29 se produce una "Violación de la confidencialidad" cuando se produce una revelación no autorizada o accidental de los datos personales, o el acceso a los mismos.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en el artículo 32 del RGPD, que reglamentan la seguridad del tratamiento.

III
Artículo 5.1.f) del RGPD

Establece el artículo 5.1.f) del RGPD lo siguiente:

"Artículo 5 Principios relativos al tratamiento:

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 relación con este principio, el Considerando 39 del referido RGPD señala que:

"[…]Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".

La documentación obrante en el expediente ofrece indicios evidentes de que la parte reclamada vulneró el artículo 5.1 f) del RGPD, *principios relativos al tratamiento* toda vez que, a raíz de la brecha de confidencialidad, los datos personales de (…) personas obrantes en el fichero fueron indebidamente expuestos a terceros, vulnerando los principios de integridad y confidencialidad, ambos establecidos en el citado artículo 5.1.f) del RGPD.

Los datos afectados por la vulneración detectada fueron: (…).

De conformidad con las evidencias de las que se dispone en el presente momento de acuerdo de inicio del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 5.1.f) del RGPD.

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

De confirmarse, la citada infracción del artículo 5.1.f) del RGPD podría suponer la comisión de las infracciones tipificadas 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
Artículo 32 del RGPD

Establece el artículo 32 del RGPD, *seguridad del tratamiento*, lo siguiente:

"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".

Los hechos puestos de manifiesto suponen la falta de medidas técnicas y organizativas al posibilitar la exhibición de datos de carácter personal de los usuarios registrados, trabajadores de la empresa, con la consiguiente falta de diligencia por el responsable, permitiendo el acceso no autorizado por terceros ajenos. El responsable del tratamiento sostiene que la vulnerabilidad se debió a un error de programación durante el desarrollo de unas pruebas de la nueva versión de la intranet corporativa, por uno de los técnicos informáticos (programador junior) que insertó accidentalmente un enlace que permitía la descarga del fichero.

En su momento, cumpliendo con la obligación de facilitar a los trabajadores un "certificado de autorresponsabilidad Covid-19", se programó un formulario autorrellenable de autorización de movimiento del personal en horario de restricción COVID-19.

En principio dicho formulario, sólo era accesible para los usuarios registrados, trabajadores de la empresa, no conteniendo datos personales, hasta que fuese rellenado por los propios trabajadores.

Del análisis de la documentación aportada por la parte reclamada, resulta que fue esta base de datos, la que alimentó, con datos reales, el fichero al que se accedía de forma accidental. Este escenario representa un gran riesgo que puede terminar propiciando la fuga de la información a terceros. El riesgo se halla, precisamente, cuando se utilizan datos reales de aquellas personas que estaban en la base de datos del entorno productivo -un lugar donde se encontraban seguros- y se pasan al entorno de prueba donde están más vulnerables. De ahí que deba asegurarse que los datos sean reemplazados por otros, de forma que puedan ser utilizados en entornos de pruebas, con la seguridad de que las pruebas sean válidas, mientras se garantiza la protección de los datos confidenciales de manera que, si estos llegasen a fugarse, no exista la posibilidad de relacionarlos con las personas reales en cuestión. Es una medida de seguridad básica, reflejo del principio de privacidad desde el diseño y por defecto.

Asimismo, consta que, aunque el error de programación que ha causado la brecha de seguridad es improbable que hubiera sido detectado en una batería de pruebas, el encargado del tratamiento no ha proporcionado evidencias que constaten que en este caso se haya efectuado la batería de pruebas antes de llevar la versión a producción. La fase de pruebas es un proceso necesario y muy importante que, de llevarse a cabo correctamente, constituye otra medida de seguridad que permite obtener resultados

fiables, siendo de gran provecho para la empresa en cuestión para operar de forma más eficiente.

En este sentido, el encargado del tratamiento se ha comprometido a encargar dichas labores a un programador senior con más de años de experiencia.

Hay que señalar que el RGPD en el citado precepto 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.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

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

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

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."

En este sentido, la búsqueda en internet, por ejemplo, (…) puede ofrecer resultados que combinándolos con los ahora accedidos por terceros, nos permitan el acceso a otras aplicaciones de los afectados o la creación de perfiles de personalidad, que no tienen por qué haber sido consentida por su titular.

La responsabilidad del reclamado viene determinada por la falta de medidas de seguridad, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

En este sentido, el Considerando 74 del RGPD establece que:

"Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas."

Trasladando estas consideraciones al caso concreto que se examina, se puede concluir que, en el momento de producirse la brecha, la parte reclamada no disponía de las medidas de seguridad razonables en función de los posibles riesgos estimados, puesto que la propia reclamada reconoce que el enlace de acceso al archivo se pegó por error en el logo de la página de acceso a la intranet corporativa por uno de los técnicos informáticos (programador junior) habiendo solicitado desde entonces el traslado de la dirección y supervisión de la programación, mantenimiento y pruebas de la intranet Serviap a un programador senior con más años de experiencia.

De conformidad con las evidencias de las que se dispone en este acuerdo de iniciación del procedimiento sancionador, y sin perjuicio de lo que resulte de la

instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a la reclamada, por vulneración del artículo 32 del RGPD

VI
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 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 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."

VII
Propuesta de sanción

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan**:**

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el

artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida; i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42,
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción."

Por su parte, el artículo 76 "*Sanciones y medidas correctivas" de la LOPDGDD* dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo con lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos

supuestos en los que existan controversias entre aquellos y cualquier interesado."

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

De acuerdo con los preceptos transcritos, y sin perjuicio de lo que resulte de la instrucción del procedimiento, a efectos de fijar el importe de la sanción por infracción del artículo 5.1 f) del RGPD, a la parte reclamada como responsable de la citada infracción tipificada en el artículo 83.5 del RGPD, procede graduar la multa teniendo en cuenta:

Como agravantes:

Artículo 83.2 a) *la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;* por no haber garantizado debidamente, al menos entre finales de noviembre y principios de diciembre de 2021, la confidencialidad de los datos de (…) personas afectadas. La propia reclamada reconoce que el enlace de acceso al archivo se pegó por error en el logo de la página de acceso a la intranet corporativa.

Considerando los factores expuestos, la valoración inicial que alcanza la cuantía de la multa es de 20.000 € por infracción del artículo 5.1 f) del RGPD, respecto a la vulneración del principio de confidencialidad.

Sanción por la infracción del artículo 32 del RGPD

De acuerdo con los preceptos transcritos, y sin perjuicio de lo que resulte de la instrucción del procedimiento, a efectos de fijar el importe de la sanción por infracción del artículo 32 del RGPD, a la parte reclamada como responsable de la citada infracción tipificada en el artículo 83.4 del RGPD, procede graduar la multa teniendo en cuenta:

Como agravantes:

Artículo 83.2 a) *la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;* por no haber garantizado debidamente, al menos entre finales de noviembre y principios de diciembre de 2021, la confidencialidad de los datos de (…) personas afectadas. La propia reclamada reconoce que el enlace de acceso al archivo se pegó por error en el logo de la página de acceso a la intranet corporativa.

Considerando los factores expuestos, la valoración inicial que alcanza la cuantía de la multa es de 10.000 € por infracción del artículo 32 del RGPD, respecto a la falta de diligencia a la hora de implementar las medidas apropiadas de seguridad.

Por lo tanto, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a BARNA PORTERS SEGURETAT, S.L., con NIF B62735089,

- por la presunta infracción del artículo 5.1.f) del RGPD, tipificada conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1 a) de la LOPDGDD.

- por la presunta infracción del artículo 32 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del RGPD, calificada como grave a efectos de prescripción en el artículo 73 f) de la LOPDGDD.

SEGUNDO: NOMBRAR instructor a ***B.B.B.*** y, como secretario, a ***C.C.C.***, indicando que cualquiera de ellos podrá ser recusado, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

TERCERO: INCORPORAR al expediente sancionador, a efectos probatorios, la reclamación interpuesta por la parte reclamante y su documentación, la documentación aportada por BARNA PORTERS SEGURETAT, S.L., con NIF B62735089, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería, por la supuesta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 de dicha norma, multa administrativa de cuantía 20.000,00 euros y por la supuesta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 10.000,00 euros.

QUINTO: NOTIFICAR el presente acuerdo a BARNA PORTERS SEGURETAT, S.L., con NIF B62735089, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en 24.000,00 euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en 24.000,00 euros y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en 18.000,00 euros.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (24.000,00 euros o 18.000,00 euros), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para continuar con el procedimiento en concordancia con la cantidad ingresada.

El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

En cumplimiento de los artículos 14, 41 y 43 de la LPACAP, se advierte de que, en lo sucesivo, las notificaciones que se le remitan se realizarán exclusivamente de forma electrónica, a través de la Dirección Electrónica Habilitada Única (dehu.redsara.es) y el Servicio de Notificaciones Electrónicas (notificaciones.060.es), y que, de no acceder a ellas, se hará constar su rechazo en el expediente, dando por efectuado el trámite y siguiéndose el procedimiento. Se le informa que puede identificar ante esta Agencia una dirección de correo electrónico para recibir el aviso de puesta a disposición de las notificaciones y que la falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

935-080323

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

>>

SEGUNDO**:** En fecha 13 de abril de 2023, la parte reclamada ha procedido al pago de la sanción en la cuantía de **18000 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

TERCERO**:** El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio.

FUNDAMENTOS DE DERECHO

I
Competencia

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
Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"*1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.*

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

De acuerdo con lo señalado,
la Directora de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la terminación del procedimiento **EXP202201318**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a ***BARNA PORTERS SEGURETAT, S.L.***.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer 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 de julio, 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.

936-040822

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