- **Expediente N.º: PS/00166/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: En fecha 3 de febrero de 2021, ALTERNATIVA SINDICAL DE TRABAJADORES DE SEGURIDAD PRIVADA (en adelante, la parte reclamante), interpuso reclamación ante la Agencia Española de Protección de Datos, contra EULEN SEGURIDAD, S.A. con NIF A28369395 (en adelante, la parte reclamada).

La parte reclamante manifiesta que la entidad reclamada está revelando el número de DNI del personal que desempeña sus funciones en las oficinas del Centro de Formación de Los Cármenes (Agencia para el Empleo del Ayuntamiento de Madrid) a través de la nota informativa de utilización del vestuario del centro de trabajo, que han de firmar los empleados.

La afectada, que ha planteado la reclamación en nombre del sindicato ALTERNATIVA SINDICAL, en calidad de delegada sindical, considera que un dato como el DNI puede ser utilizado por otras personas de forma fraudulenta o con otros fines distintos para los que está siendo tratado, por lo que no debe exponerse de esta forma, a la vista de otros trabajadores de la empresa o del cliente (p.ej. recepcionistas, limpieza, otros compañeros...).

Expone que no sólo no se está solicitando su consentimiento para dicho tratamiento, sino que, además, se les está apremiando para obtener el documento ya firmado.

Aporta imagen de la nota informativa en cuestión y captura de pantalla de los correos electrónicos de la reclamante con el Gestor de Servicio de la empresa, donde éste solicita la mencionada nota ya firmada.

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 al reclamado, 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.

En fecha 31 de marzo, se recibe en esta Agencia escrito de respuesta, si bien la empresa no aclara el motivo de exponer el número de DNI completo de los empleados que han de firmar la hoja con las nuevas condiciones, permitiendo a cada uno de ellos tener acceso al identificador de los que han firmado antes, en un documento cuya custodia final corresponde a la empresa que está recogiendo la información. Asimismo, manifiesta que es una comunicación de datos amparada en la relación contractual, que el documento se encontraba de forma temporal en una zona restringida con las debidas medidas de seguridad a la que solo tenía acceso el personal de seguridad y que a raíz de esta reclamación, se está valorando la

posibilidad de que, en el caso de que fuese necesario publicar un D.N.I, se cumpla con la disposición adicional séptima de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

TERCERO: En fecha 8 de abril de 2021, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra el reclamado.

CUARTO: En fecha 18 de agosto de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del artículo 5.1.f) del RGPD y artículo 32 del RGPD, tipificada en el artículo 83.5 y 83.4 del RGPD, respectivamente.

QUINTO: Notificado el acuerdo de inicio, la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifestaba que el incidente se produjo por un error humano motivado principalmente por la urgencia en notificar las medidas que debían adoptarse tras eliminar el sistema de ventilación, que se ha tratado de un supuesto accidental y fortuito que ha quedado encuadrado dentro del ámbito interno de la empresa, que el volumen de datos y la tipología de los datos afectados ha sido mínima, que no ha tenido ninguna consecuencia para el reclamante ni para los empleados del servicio, que los datos sólo fueron visibles durante un periodo corto de tiempo y que se han tomado medidas preventivas para evitar este tipo de casos, y solicita el archivo de la reclamación presentada y en su defecto el sobreseimiento del presente expediente sancionador

SEXTO: En fecha 9 de diciembre de 2021 se formuló propuesta de resolución, proponiendo:

<<Que por la Directora de la Agencia Española de Protección de Datos se sancione a EULEN SEGURIDAD S.A., con NIF A28369395, por una infracción del artículo 5.1.f) del RGPD y artículo 32 del RGPD, tipificada en el artículo 83.5 del RGPD, con una multa de TRES MIL EUROS (3,000 €)>>

SÉPTIMO: En fecha 23 de diciembre de 2021, la parte reclamada presenta escrito de alegaciones a la Propuesta de resolución, en el que, en síntesis, manifiesta que, en caso de conocimiento, se hubiesen tomado todas las acciones necesarias y activado los correspondientes procedimientos para minimizar la incidencia e implantar acciones correctivas a la misma, que el presente incidente no ha acarreado una pérdida de disposición y control sobre los datos personales, ya que los mismos se encontraban perfectamente localizados y dentro de un entorno securizado, que no ha entrañado un riesgo para los derechos de los afectados en la medida que se tuvo un acceso limitado y temporal a datos de carácter personal básicos (no pertenecen a categorías especiales de datos), dentro de un entorno laboral y de confianza y no ha supuesto ningún perjuicio para los afectados transcurrido un año, expone que se han aplicado las medidas de seguridad de acuerdo con los riesgos definidos y que el empleado incluyó por error el documento de identidad, saltándose los procedimientos internos, dada la urgencia del caso y la situación derivada del COVID, por lo que solicita el archivo de la reclamación presentada en su día.
A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS PROBADOS

PRIMERO: En fecha 3 de febrero de 2021, la parte reclamante interpuso reclamación ante la Agencia Española de Protección de Datos, manifestando que la entidad reclamada estaba revelando el número de DNI de los empleados de la empresa a través de una nota informativa que debían firmar.

SEGUNDO: Comprobada la documentación aportada y que se encuentra incorporada al expediente, consta que terceros ajenos tuvieron acceso no autorizado a datos de carácter personal de empleados de la empresa.

TERCERO: La parte reclamada reconoce que el documento se encontraba de forma temporal en una zona restringida con las debidas medidas de seguridad a la que solo tenía acceso el personal de seguridad y que, a raíz de esta reclamación, se está valorando la posibilidad de que, en el caso de que fuese necesario publicar un D.N.I, se cumpla con la disposición adicional séptima de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

CUARTO: En la actualidad parte reclamada expone que ha procedido a implantar las medidas correctoras adecuadas para evitar la repetición de hechos similares en el futuro.

FUNDAMENTOS DE DERECHO

PRIMERO: 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 y 48.1 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*."

SEGUNDO: Respecto a las alegaciones presentadas a la Propuesta de Resolución, se debe señalar lo siguiente:

En primer lugar, de los hechos probados en este procedimiento se desprende que la visualización de los datos de carácter personal por parte terceros ajenos, permiten constatar que la parte reclamada no ha podido garantizar la seguridad adecuada en el tratamiento de los datos personales de los empleados de la empresa, incurriendo por ello en la vulneración del artículo 5.1 f) del RGPD, que rige los principios de integridad y confidencialidad de los datos personales, así como la responsabilidad proactiva del responsable del tratamiento de demostrar su cumplimiento.

En el caso concreto que se examina, los hechos reclamados se concretan en la distribución de una nota informativa entre los empleados, que debían rellenar con su

nombre, apellidos, DNI y firma, permitiendo el acceso entre ellos, al identificador de los que habían firmado antes. Es decir, la empresa tenía habilitación para tratar internamente y conocer determinada información, pero no estaba legitimada para transferirla a terceros.

En este sentido se debe señalar que el DNI unido al nombre y apellido de la persona es considerado como un dato personal, tanto por el RGPD como por la LOPDGDD. Y es así porque a través de este, podría identificarse a una persona y al ser un dato personal, deben aplicarse las mismas medidas de protección que sobre otros datos personales.

Tanto el RGPD como la LOPDGDD tienen por objeto garantizar los derechos fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales amparado por el artículo 18 de la Constitución. De esta forma, cualquier dato personal que la empresa pueda tratar en relación con los trabajadores, queda protegido por la normativa de protección de datos personales mediante la aplicación de una serie de principios y garantías que resultan exigibles en relación con cualquier tratamiento que se realice.

En segundo lugar, en cuanto al argumento de que el incidente no ha acarreado una pérdida de disposición y control sobre los datos personales, ya que los mismos se encontraban perfectamente localizados y dentro de un entorno securizado, que no ha entrañado un riesgo para los derechos de los afectados en la medida que se tuvo un acceso limitado y temporal a datos de carácter personal básicos (no pertenecen a categorías especiales de datos), dentro de un entorno laboral y de confianza y no ha supuesto ningún perjuicio para los afectados transcurrido un año, no es causa de justificación o exculpación suficiente, toda vez que los afectados se han visto desprovistos del control sobre sus datos personales.

En este caso la búsqueda en internet, por ejemplo, del nombre, apellidos de alguno de los afectados puede ofrecer resultados que combinándolos con los ahora accedidos por terceros ajenos, 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.

Esta posibilidad supone un riesgo añadido que se ha de valorar y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

El hecho de que fue un empleado el que incluyó por error el documento de identidad, saltándose los procedimientos internos, dada la urgencia del caso y la situación derivada del COVID, hay que señalar que las medidas de seguridad deben adoptarse en atención a todos y cada uno de los riesgos presentes en un tratamiento de datos de carácter personal, incluyendo entre los mismos, el factor humano. Este riesgo debe ser tenido en cuenta por el responsable del tratamiento que, en función de este, debe establecer las medidas técnicas y organizativas necesarias que impida la pérdida de control de los datos por parte del responsable del tratamiento y, por tanto, por parte de los titulares de los datos que se los proporcionaron.

En consecuencia, las alegaciones deben ser desestimadas, significándose que las argumentaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

TERCERO: El artículo 5.1.f) del RGPD, Principios relativos al tratamiento, establece lo siguiente:

"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»)".

El artículo 5 de la LOPDGDD, Deber de confidencialidad, señala lo siguiente:

"1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3.Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento".

La documentación obrante en el expediente acredita que la parte reclamada vulneró el artículo 5 "Principios relativos al tratamiento" del RGPD, apartado 1.f), en relación con el artículo 5 "Deber de confidencialidad" de la LOPGDD, al revelar información y datos de carácter personal a terceros.

Este deber de confidencialidad, con anterioridad deber de secreto, debe entenderse que tiene como finalidad evitar esas filtraciones de los datos no consentidas por los titulares de estos. Se trata de una obligación que incumbe al responsable y encargado del tratamiento, así como a todo aquel que intervenga en cualquier fase del tratamiento; y que es complementaria del deber de secreto profesional.

CUARTO: 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 (El subrayado es de la AEPD).

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 el presente caso, como consecuencia de una falta de implantación de medidas técnicas y organizativas ha provocado el acceso por terceros no autorizados a los datos personales de empleados de la empresa.

De las actuaciones practicadas consta la existencia de indicios razonables y suficientes de que las medidas de seguridad, tanto de índole técnica como

organizativas, con las que contaba la parte reclamada en relación con los datos que sometía a tratamiento, no eran adecuadas al momento de producirse la brecha de seguridad, vulnerando con ello el artículo 32 del RGPD.

La consecuencia de esta falta de medidas de seguridad fue la exposición a terceros ajenos de los datos personales de empleados de la empresa. Es decir, los afectados se han visto desprovistos del control sobre sus datos personales.

Como se ha indicado anteriormente, en este caso la búsqueda en internet, por ejemplo, del nombre, apellidos, DNI o correo electrónico de alguno de los afectados 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.

Esta posibilidad supone un riesgo añadido que se ha de valorar en el estudio de gestión de riesgos y que aumenta la exigencia del grado de protección en relación con la seguridad y salvaguarda de la integridad y confidencialidad de estos datos.

Este riesgo debe ser tenido en cuenta por el responsable del tratamiento quien debe establecer las medidas técnicas y organizativas necesarias que impida la pérdida de control de los datos por el responsable del tratamiento y, por tanto, por parte de los titulares de los datos que se los proporcionaron.

QUINTO: El artículo 83.5 del RGPD, dispone lo siguiente:

"5. 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;"

Por su parte, el artículo 71 de la LOPDGDD, bajo la rúbrica "*Infracciones*" determina lo siguiente: "*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 de las infracciones, el artículo 72 de la LOPDGDD, bajo la rúbrica de infracciones consideradas muy graves, establece lo siguiente: *"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:*

(…)

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

La vulneración del artículo 32 RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. 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 de las infracciones, el artículo 73 de la LOPDGDD, establece bajo la rúbrica *"Infracciones consideradas graves",* lo siguiente:

"*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.

En el presente caso, concurren las circunstancias infractoras previstas en el artículo 83.5 y 83.4 del RGPD arriba transcritos.

SEXTO: 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 naturale-

za, 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."

De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción por infracción del artículo 5.1 f) y 32 del RGPD, a la parte reclamada como responsable de las citadas infracciones procede graduar la multa teniendo en cuenta:

-La intencionalidad o negligencia apreciada en la infracción: en el presente caso, consta una grave negligencia en la conducta al exponer datos de carácter personal de empleados de la empresa a terceros ajenos que tuvieron acceso no autorizado a dichos datos.

-La vinculación de la actividad del infractor con la realización de tratamientos de datos personales, ya que la actividad empresarial de la reclamada exige un continuo tratamiento de datos de carácter personal tanto de clientes como de terceros, ya que se trata de una de las mayores empresas del país en su sector de negocio o actividad.

Paralelamente, concurren como atenuantes los siguientes criterios:

Artículo 83.2.c) RGPD: *cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados*

Artículo 83.2.h) RGPD*: 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.*

En el presente caso, el reclamado ha informado a esta Agencia de las circunstancias en las que se produjo la incidencia que propició la reclamación, así como las medidas a adoptar a fin de evitar que hechos como el reclamado vuelvan a producirse en el futuro.

Artículo 83.2 k) RGPD: cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso. Asimismo, se considera que la respuesta ha sido razonable, re-

conociendo los hechos, no teniéndose constancia de otras reclamaciones por parte de las personas afectadas.

Considerando los factores expuestos, la valoración que alcanza la cuantía de la multa es de 2.000 € por infracción del artículo 5.1 f) del RGPD, respecto a la vulneración del principio de confidencialidad y de 1.000 € por infracción del artículo 32 del citado RGPD, respecto a la seguridad del tratamiento de los datos personales.

SÉPTIMO: Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los "*Principios de la Potestad sancionadora*", en el artículo 28 la bajo la rúbrica "*Responsabilidad*", lo siguiente:

"1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

La falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad constituye el elemento de la culpabilidad.

OCTAVO: El artículo 70.1 de la LOPDGDD señala los sujetos responsables.

"1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

a) Los responsables de los tratamientos."

De las evidencias de las que se dispone conforme a los hechos probados en el presente procedimiento sancionador, consta acreditada la infracción de los artículos 32 y 5.1.f) del RGPD, en los términos antes descritos.

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: IMPONER a EULEN SEGURIDAD S.A., con NIF A28369395, por una infracción del artículo 5.1.f) del RGPD, tipificada en el art. 83.5 del RGPD, y por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD, respectivamente, una multa de 2.000 € (dos mil euros) y una multa de 1.000€ (mil euros). Ello hace un total de 3.000€ (tres mil euros).

SEGUNDO: NOTIFICAR la presente resolución a EULEN SEGURIDAD S.A.

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el

art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº ***ES00 0000 0000 0000 0000 0000***, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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 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.

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 de octubre. 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.

938-270122

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