

- **Expediente N.º: EXP202311138**

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 16 de enero de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **CENTRAL SINDICAL INDEPENDIENTE Y DE FUNCIONARIOS CSI- CSIF** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202311138

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: **A.A.A., B.B.B., C.C.C., D.D.D., E.E.E. y F.F.F.** (en adelante, las partes reclamantes) con fecha 4 de julio de 2023 interpusieron reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **CENTRAL SINDICAL INDEPENDIENTE Y DE FUNCIONARIOS CSI- CSIF** con NIF **G79514378** (en adelante, la parte reclamada).

En dichos escritos, las partes reclamantes manifestaban que, en fecha 12 de mayo de 2023, representantes de la parte reclamada remitieron un correo electrónico con destino a todo el personal del Área Sanitaria de Ferrol del Servicio Gallego de Salud (SERGAS). Afirma que en dicho correo se adjuntaba el acta global de escrutinio para las Juntas de Personal en las elecciones sindicales celebradas en mayo de 2023, donde se muestran los datos identificativos (nombre, apellidos y DNI) de quienes actuaron como interventores de mesa, así como de los representantes elegidos, entre los cuales se encuentran las partes reclamantes, sin consentimiento previo de estas.

A efectos acreditativos, aportan junto a sus reclamaciones copia del correo electrónico remitido y de la documentación adjunta al mismo, consistente en acta global de escrutinio. En dicha acta se comprueba la existencia de determinados datos personales sin anonimizar:

- Nombre, apellidos, DNI y sexo de los representantes elegidos, así como el sindicato, coalición o grupo al que pertenecen.
- Nombre apellidos, DNI de las personas que formaron parte de la mesa electoral coordinadora, así como el cargo en dicha mesa (interventor/a, presidente/a o secretario/a)

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), fue recogido en fecha 11/08/2023 como consta en el acuse de recibo que obra en el expediente.

Con fecha 07/09/2023 se recibe en esta Agencia escrito de respuesta por la parte reclamada. La información recibida se centraba principalmente en las medidas y protocolos implementados en respuesta a la solicitud de la presente autoridad.

Dicho escrito se inicia con recomendaciones del Delegado de Protección de Datos de la parte reclamada, aconsejando el uso de herramientas y correos electrónicos corporativos con el fin de asegurar la seguridad de los datos en comunicaciones electrónicas, especialmente en el contexto de procesos electorales sindicales. Se resalta la importancia del cifrado de la información para mantener su confidencialidad e integridad, así como la utilización de la opción de copia oculta en correos electrónicos con el fin de proteger las direcciones de correo de los destinatarios. Además, se advierte sobre la necesidad de evitar la cesión de datos personales a terceros sin justificación legal.

En cuanto a las herramientas para el envío masivo de correo, la parte reclamada afirma disponer de una aplicación de gestión de afiliados y una plataforma específica para estos envíos. Estas herramientas incluyen diversas medidas, entre las cuales se encuentra la inclusión de un enlace en los correos para que los destinatarios puedan darse de baja en futuros envíos. Se presta especial atención en adjuntar los archivos a un servidor y compartir el enlace desde el mismo, evitando adjuntar directamente en los correos, facilitando de esta forma el control y la seguridad de la información que se pretende compartir.

Se menciona asimismo la realización de investigaciones para determinar la extensión y la autoría de los hechos relacionados con la reclamación. En este sentido, se pone de manifiesto la necesidad de incrementar la formación y sensibilización del personal en la protección de datos personales, con especial atención en los delegados, quienes a su juicio podrían haber cometido el error de compartir información personal sin base jurídica. A tal respecto, se indica que la causa de la incidencia que originó la reclamación parece ser un trato inadecuado de los datos personales de dichos delegados, que no siguieron las directrices marcadas por la parte reclamada. En relación a dicho hecho, sugiere que la información publicada en la intranet de la

Administración relativa a un acta anterior de elecciones sindicales pudo haber inducido a error.

En cuanto a las medidas adoptadas para prevenir incidentes similares, se indica que se han adoptado varias de ellas, como la sensibilización y concienciación sobre los protocolos de protección de datos o la designación de responsables en cada unión provincial con el fin de solventar consultas o cuestiones planteadas en materia de protección de datos.

Finalmente, se hace referencia a las particularidades que poseen las organizaciones sindicales, especialmente en lo que respecta al rol que poseen los delegados sindicales en los centros de trabajo, donde la implementación de medidas de seguridad, afirman, puede resultar más complicada. A pesar de dichas dificultades, la parte reclamada muestra su compromiso con la supervisión y el cumplimiento de las normas de protección de datos.

Como conclusión, la parte reclamada solicita que, en base a la información y documentación proporcionada, se proceda al archivo del presente caso.

TERCERO: Con fecha 4 de octubre de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

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

Obligación incumplida del artículo 5.1 f) RGPD

De acuerdo con el apartado 1.f) del artículo 5 RGPD los datos deben ser *"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»)"*

De la misma forma, el Considerado 39 RGPD dispone 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.”*

El principio de confidencialidad, según el mencionado artículo 5.1 f) del RGPD, exige la protección de datos personales contra accesos, usos y divulgaciones no autorizados. Dicho principio resulta esencial para garantizar la seguridad de los datos personales, constituyendo un pilar clave en dicha materia. Por el contrario, la violación de este principio puede tener consecuencias no deseadas, reflejándose su importancia en el marco normativo de la protección de datos.

En el presente supuesto, el hecho denunciado por los reclamantes consistente en el envío de un correo electrónico con el acta global de escrutinio donde se incluían nombres, apellidos, DNI y datos relativos a la sindicación, de los representantes elegidos y de las personas que formaron parte de la mesa electoral constituye una presunta violación del mencionado principio de confidencialidad.

A tal respecto, resulta conveniente señalar el artículo 4 del RGPD el cual define como datos personales *“a toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.”*

No cabe duda de que los datos correspondientes al nombre, apellidos y DNI, tanto de los representantes elegidos como de las personas que formaron parte de la mesa, se trata de información que permite la identificación directa de dichas personas por lo que deben considerarse como datos personales en los términos indicados por dicho artículo.

Especial atención merece los datos relativos a la organización sindical correspondiente a los representantes que asimismo aparecen en el acta objeto de la presente reclamación. A tal respecto, el artículo 9 del RGPD relativo a las categorías especiales de datos personales establece que *“Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.”*

De la lectura de dicho artículo se deriva por parte del RGPD una protección reforzada para ciertas categorías especiales de datos personales considerados particularmente sensibles, entre los cuales se encuentran los datos sobre la afiliación sindical de una persona. Dichos datos requieren mayores garantías, entre otros motivos, debido a su potencialidad para ser utilizados de forma discriminatoria o perjudicial por lo que, como regla general, se requiere un nivel de exigencia más alto que para el resto de los datos personales.

En el caso que nos ocupa, la divulgación conjunta de los datos de identificación junto a los datos de afiliación sindical expone a los individuos a posibles daños que justifican esta especial protección, como la discriminación o el tratamiento injusto basado en su pertenencia a una determinada organización sindical. Teniendo en cuenta dichas circunstancias, en el supuesto de infracción de este principio la gravedad es mayor, pues implica riesgos significativos para los derechos y libertades de las personas afectadas.

Por otro lado, el artículo 4 del RGPD define al «responsable del tratamiento como *“aquella la persona física o jurídica, autoridad, 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”*.

En este sentido, conviene resaltar que la responsabilidad de la divulgación de los datos objeto de reclamación corresponde a la organización sindical, en su condición de responsable de tratamiento y no a los delegados sindicales que enviaron el correo donde se contenían dichos datos, pues es aquella la que ha determinado los fines y medios del tratamiento.

Dicha afirmación, se sustenta en la jurisprudencia establecida por el Tribunal Constitucional (entre otras, sentencias STC 61/1989 y STC 208/1993), según la cual los delegados sindicales son considerados instancias organizativas internas del sindicato en la empresa. En virtud de dicha doctrina, los delegados sindicales no solo desempeñan funciones representativas del sindicato en la empresa, como la negociación colectiva o la resolución de conflictos colectivos, sino que también trasladan al sindicato la responsabilidad legal que se genere por su actividad.

Por lo expuesto, y sin perjuicio de lo que resulte a lo largo del presente procedimiento, la exposición de datos personales de las partes reclamadas implica una presunta vulneración del principio de confidencialidad de los datos personales reconocido en el artículo 5.1 f) del RGPD.

III

Tipificación y calificación 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. (...)”

IV

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

Según el artículo 83.2 del RGPD *“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, y*
- 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”*.

Teniendo en cuenta dichos preceptos, en el presente supuesto se considera que procede graduar la sanción a imponer en los siguientes términos:

Posible agravante prevista en el apartado g) del artículo 83.2 del RGPD:

g) las categorías de los datos de carácter personal afectados por la infracción;

La inclusión del citado agravante se fundamenta jurídicamente en la naturaleza de los datos que fueron expuesto en el presente caso, entre los cuales se encontraban datos sindicales, considerados como categoría especial de datos personales en los términos establecidos por el artículo 9 del RGPD. La exposición de datos de dicha naturaleza intensifica la gravedad de la infracción, debido a la mayor vulnerabilidad y los riesgos asociados ante un posible tratamiento indebido o inadecuado.

No se aprecia la concurrencia de circunstancias atenuantes.

En función de las mencionadas circunstancias, de acuerdo con lo dispuesto en el artículo 83.5 del RGPD, y sin perjuicio de lo que resulte de la instrucción del presente procedimiento, se considera adecuado fijar como posible sanción una multa de cuantía de 3.000 € (TRES MIL EUROS)

V

Artículo 32 del RGPD

El artículo 32 “Seguridad del tratamiento” del RGPD establece:

“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”.

Resulta necesario señalar que el citado precepto no establece un listado de medidas de seguridad concretas de acuerdo con los datos objeto de tratamiento, sino que establece la obligación de que el responsable y el encargado del tratamiento apliquen 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, determinando aquellas medidas técnicas y organizativas adecuadas 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 debe tener 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.

Por su parte, 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”.

En el presente caso, los hechos objeto de las distintas reclamaciones ponen de manifiesta una inadecuación de las medidas técnicas y organizativas adoptadas para garantizar un nivel de seguridad adecuado al riesgo. Si bien la parte reclamada ha acreditado la implementación de ciertas medidas, el incidente producido pone de manifiesto que esas medidas han resultado ser ineficaces, lo cual muestra una

inadecuación entre la implementación de las políticas de seguridad de datos y su efectividad práctica.

De forma concreta, de la documentación obrante en el momento de la redacción del presente acuerdo, se desprende que la entidad no ha implementado medidas efectivas para asegurar que las personas que se encuentran a su cargo y que tienen acceso a datos de carácter personal traten dichos datos siguiendo las instrucciones del responsable, tal y como prevé de forma expresa el apartado cuarto del artículo 32. Ello deriva de la propia manifestación de la parte reclamada al indicar que la causa de la incidencia que originó las reclamaciones se debió a un trato inadecuado de los datos personales de los delegados sindicales, que no siguieron las directrices marcadas por la parte reclamada.

Dicha previsión legal es consecuencia del principio de responsabilidad proactiva y asegura una adecuada coherencia entre la implementación de las medidas adoptadas por el responsable del tratamiento y la efectividad de las mismas en el tratamiento que realizan las personas que se encuentran a su cargo en cualquier organización. De esta forma, se logra evitar un acceso no autorizado o el tratamiento inadecuado de los datos personales, garantizando la protección y la confidencialidad de la información.

En cuanto a las medidas efectivas para garantizar la exigencia de que los datos personales se traten únicamente siguiendo las instrucciones del responsable, va a depender de la naturaleza y la estructura de la organización, si bien a modo meramente ejemplificativo, pueden mencionarse las siguientes:

- Formación regular y específica sobre protección de datos y RGPD a todo el personal de la organización, incluyendo los delegados sindicales. Este tipo de formación debería incluir instrucciones claras sobre el tratamiento de datos personales en la organización, la importancia de su seguimiento y las consecuencias de no hacerlo. De hecho, respecto a esta cuestión, la propia parte reclamada ha puesto de manifiesto de forma expresa la necesidad de incrementar la formación y sensibilización del personal en la protección de datos personales; especialmente la dirigida a los delegados.
- Control de acceso: Mediante la implementación de sistemas de control que limiten el acceso a datos personales solo a aquel personal que necesita acceder a dichos datos para realizar sus funciones. Ello implica una adecuada delimitación de las funciones del personal, incluidas la de los propios delegados, determinando si tratan o no datos personales.
- Auditorías y supervisión regular: Realizar auditorías periódicas permite también asegurar el cumplimiento de las instrucciones adoptadas por el responsable o el encargado del tratamiento. Dicho resultado debe ir acompañado, además, de advertencias o recomendaciones a todo el personal para evitar posibles desviaciones respecto las instrucciones indicadas.
- Respuestas a incidentes. Para ello resulta apropiado desarrollar y mantener un plan de acción para dar respuesta a los posibles incidentes que pueden surgir. Ello permite evitar, en caso de incumplimiento, que el mismo vuelva a producirse y otorga una mayor concienciación de la importancia del seguimiento de las citadas instrucciones por parte del personal.

Debe de tenerse en cuenta que la utilización de las mencionadas medidas u otras que se consideran oportunas por parte del responsable resultarán eficaces cuando únicamente cumplan el objetivo de garantizar lo indicado en el apartado cuarto del artículo 32, esto es, garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado pueda tratar los datos personales a los que tengan acceso siguiendo las instrucciones del responsable. Si, por el contrario, a pesar de su adopción, no han resultado eficaces, dichas medidas no son adecuadas y, por tanto, se habrá incumplido la obligación exigida por el artículo, como ocurre en el presente caso.

En este supuesto, además, la no adopción de las medidas adecuadas se agrava teniendo en cuenta la naturaleza de los datos personales tratados por la parte reclamada, puesto que las organizaciones sindicales tratan regularmente categorías especiales de datos previstos en el artículo 9 del RGPD como, por ejemplo, la afiliación sindical. Ello exige un nivel más alto de protección y cautela, lo que incluye la implementación de medidas técnicas y organizativas avanzadas para asegurar su confidencialidad e integridad.

A ello debe añadirse que en entidades de esta naturaleza se suelen tratar una gran cantidad de datos personales, no solo de sus miembros, sino también de otras personas implicadas en diversas actividades sindicales. En este sentido, la gestión de grandes volúmenes de datos aumenta la probabilidad de producción de un incidente de seguridad de datos, pues basta con uno solo para que afecte a un número considerable de individuos. Esa característica especial exige que las instrucciones indicadas por el responsable o el encargado del tratamiento sean cumplidas con mayor rigurosidad y, consecuentemente, las medidas adoptadas para garantizar el seguimiento deben de resultar adecuadas a dicha exigencia.

En conclusión, se desprende una presunta ausencia de medidas adecuadas con el fin de garantizar que el personal de la organización, incluyendo a los delegados sindicales de la misma, cumplan las instrucciones adoptadas por el responsable o el encargado del tratamiento en dicha organización. La implementación efectiva de tales medidas crea un entorno de seguridad que permite prevenir cualquier incidente que pudiera producirse. La ausencia de las mismas, por el contrario, implica un presunto incumplimiento del mencionado artículo 32, como ocurre en el presente supuesto.

Principio del formulario

VI

Tipificación y calificación 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

Posible sanción por la infracción del artículo 32 del RGPD

En los términos indicados por el mencionado artículo 83.4 del RGPD la infracción del artículo 32 se sancionará, *“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”*

No se aprecia la concurrencia de circunstancias agravantes ni atenuantes.

Teniendo en cuenta las condiciones generales para la imposición de multas administrativas establecidas por el ya mencionado artículo 83.2 del RGPD, atendiendo a las circunstancias del presente supuesto y sin perjuicio de lo que resulte de la instrucción del presente procedimiento, se propone como posible sanción una multa de cuantía de 1,000 € (MIL EUROS).

VIII

Adopción de medidas

De confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *“ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado...”*. La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

En el presente supuesto, se podrá requerir al responsable para que en un plazo de tres meses se notifique a esta autoridad la adopción de las siguientes medidas:

- Adoptar las medidas organizativas y técnicas adecuadas que eviten comunicación por cualquier medio que contengan datos personales no autorizados por parte de los miembros de la organización, incluyendo los delegados sindicales. Dichas medidas pueden consistir en una información concreta y detallada destinada a dicho personal relativa a como realizar la anonimización o cifrado de datos de forma previa a la remisión de información que contenga datos personales a través de cualquier medio.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

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 **CENTRAL SINDICAL INDEPENDIENTE Y DE FUNCIONARIOS CSI- CSIF**, con NIF **G79514378**, por la presunta infracción del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificada en el Artículo 83.5 del RGPD y Artículo 83.4 del RGPD.

SEGUNDO: NOMBRAR como instructor/a a **R.R.R.** y, como secretario/a, a **S.S.S.**, indicando que podrán ser recusados, 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, 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, sin perjuicio de lo que resulte de la instrucción:

- Por la supuesta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 de dicha norma, multa administrativa de cuantía **3.000,00 euros**

- Por la supuesta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía **1.000,00 euros**

Ello arroja una cantidad total por la presunta comisión de las infracciones de **4.000 euros (CUATRO MIL EUROS)**

QUINTO: NOTIFICAR el presente acuerdo a **CENTRAL SINDICAL INDEPENDIENTE Y DE FUNCIONARIOS CSI- CSIF**, con NIF **G79514378**, 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 expediente 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 **3.200,00 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 **3.200,00 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 **2.400,00 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.

Asimismo, con el fin de prevenir ulteriores infracciones de la misma naturaleza, el reconocimiento de responsabilidad y la consiguiente aplicación de la mencionada reducción implicará la aceptación, en su caso, de las medidas a adoptar propuestas e indicadas por esta entidad en el presente acuerdo.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (3.200,00 euros o 2.400,00 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 doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo sin que se haya dictado y notificado resolución se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

935-30102023

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

>>

SEGUNDO: En fecha 20 de enero de 2024, la parte reclamada ha procedido al pago de la sanción en la cuantía de **2400 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.

CUARTO: En el Acuerdo de inicio transcrito anteriormente se señalaba que, de confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá “ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado...”.

Habiéndose reconocido la responsabilidad de la infracción, procede la imposición de las medidas incluidas en 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 registrarán 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 **EXP202311138**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: ORDENAR a **CENTRAL SINDICAL INDEPENDIENTE Y DE FUNCIONARIOS CSI- CSIF** para que en el plazo de 3 meses desde que la presente resolución sea firme y ejecutiva, notifique a la Agencia la adopción de las medidas que se describen en los fundamentos de derecho del Acuerdo de inicio transcrito en la presente resolución.

TERCERO: NOTIFICAR la presente resolución a **CENTRAL SINDICAL INDEPENDIENTE Y DE FUNCIONARIOS CSI- CSIF**.

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.

1259-16012024

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