

- **Procedimiento N.º: PS/00077/2021**

## 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 21 de mayo de 2020, se recibe en la Agencia escrito de reclamación de D. **A.A.A.**, en el que pone de manifiesto que la web **\*\*\*URL.1** recaba datos personales pero no cumple con la normativa de protección de datos ya que no se informa del responsable del fichero ni se solicita aceptar la política de privacidad, aunque cuenta con un aviso legal situado en la dirección **\*\*\*URL.2**, únicamente se incluye: «De acuerdo con lo establecido por la normativa de Protección de Datos de Carácter Personal, le informamos que está facilitando sus datos de carácter personal al Responsable de Tratamiento Comercial de **\*\*\*URL.1**. Contacto: Email **\*\*\*EMAIL.1**».

En fecha 22 de mayo de 2020 se reciben cuatro reclamaciones de FACUA en relación con la web **\*\*\*URL.1**.

En la primera denuncia de FACUA se pone de manifiesto la falta de información en la recogida de datos. Asimismo, denuncian haber tenido conocimiento de la existencia de otra web **\*\*\*URL.3** que aparentemente se encuentra directamente relacionada con la web denunciada, y ello debido a la similitud evidente entre las direcciones URL de ambas páginas, así como en el contenido de estas. En esta web segunda se indica un número de cuenta bancaria para hacer donaciones.

En la denuncia, FACUA aporta impresiones de pantalla realizadas por la entidad e Gargante S.L. (empresa que proporciona, entre otros servicios, pruebas del contenido de una web en un momento determinado) que certifica el contenido encontrado en Internet en relación con la dirección **\*\*\*URL.1**.

En los certificados constan las fechas de 20 y 21 de mayo junto con impresiones de pantalla de un número de cuenta bancaria para hacer donativos, un formulario de contacto en el que recogen los datos de: nombre, la dirección de correo electrónico, teléfono y un mensaje.

Asimismo, consta impresión del “Aviso Legal” publicado en la web en el que informan: “De acuerdo con lo establecido por la normativa de Protección de Datos de Carácter Personal, le informamos que está facilitando sus datos de carácter personal al Responsable de Tratamiento Comercial de **\*\*\*URL.1**. Contacto: Email **\*\*\*EMAIL.1** y la legitimación del tratamiento se basa en el consentimiento al clicar el botón **ACEPTO LA POLÍTICA DE PROTECCIÓN DE DATOS**” e impresión de los “Términos y condiciones” de la web en la que se incluye un apartado de protección de datos en el que se informa **\*\*\*URL.1** se toma muy seriamente la protección de los datos de sus clientes. Estado de estos Términos y Condiciones Generales Comerciales: 21/05/2020 **\*\*\*URL.1**.

En las otras denuncias FACUA manifiesta que han comprobado que en la misma plataforma se tienen archivados toda una serie de documentos en los que se recogen datos

personales de terceros sin ninguna clase de medida de protección y se encuentran alojados en la dirección **\*\*\*URL.4** accesible por terceros

A este respecto aporta las siguientes direcciones donde se encuentran datos personales:

Correos electrónicos:

**\*\*\*URL.5**

Cuentas bancarias:

**\*\*\*URL.6**

**\*\*\*URL.7**

**\*\*\*URL.8**

Nombres y apellidos y cuentas bancarias:

**\*\*\*URL.9**

Nombres y apellidos y otros medios de pago:

**\*\*\*URL.10**

**\*\*\*URL.11**

**\*\*\*URL.12**

**\*\*\*URL.13**

**\*\*\*URL.14**

**\*\*\*URL.15**

**\*\*\*URL.16**

Nombres y apellidos:

**\*\*\*URL.17**

Adjuntan impresiones de pantalla del acceso a algunas de estas direcciones web, certificados asimismo por eGarante, que acreditan su contenido a fecha de 22 de mayo de 2020 a las 00:57:57 y a las 01:02:30. En ellas figuran datos personales nombre y apellidos, datos de pagos, justificantes de pago, números de cuentas bancarias.

Por otro lado, FACUA indica que desconoce si por parte de los responsables de la plataforma web **\*\*\*URL.1** se ha llevado a cabo notificación a la Agencia de la violación en la seguridad de los datos personales que poseen archivados, tal y como exige la normativa.

SEGUNDO: A la vista de los hechos expuestos en la reclamación, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación, teniendo conocimiento de los siguientes extremos:

ENTIDAD INVESTIGADA:

RESISTENCIA POPULAR, S.L. con CIF B67580696 y domicilio en **\*\*\*DIRECCIÓN.1**, **\*\*\*LOCALIDAD.1**, (Madrid).

Anteriormente IYANSA QUALITY SL con CIF B67580696 con domicilio en **\*\*\*DIRECCIÓN.2** (Barcelona)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN:

En fecha 25 de mayo de 2020 desde la Inspección de Datos se accede a la web **\*\*\*URL.3** verificando que en dicha web consta un apartado de *PRIVACIDAD* en el que consta como responsable del tratamiento:

Identidad: **\*\*\*URL.3**

Correo electrónico: **\*\*\*EMAIL.1**

Contacto; **\*\*\*URL.3**

Nombre del dominio: **\*\*\*URL.3**

Asimismo, se comprueba que en la web aparece un anuncio “*Estaremos de vuelta en breve*” en el que se informa que “*permanecerá cerrada durante unos días para proceder a mejoras técnicas que optimicen la experiencia de compra. Todos los pedidos que ya hayan sido realizados serán gestionados y enviados*”

En fecha 9 de junio de 2020 desde la Inspección de Datos se accede a la web **\*\*\*URL.3** verificando la existencia de un formulario de contacto en el que se solicitan los datos de: nombre, email, teléfono y mensaje con la siguiente clausula: “*El RESPONSABLE del tratamiento es IYANSA QUALITY SL domicilio en C/ **\*\*\*DIRECCIÓN.2**, BARCELONA. Fines: gestión de la solicitud, registro, compra o consulta. Puede ejercer los derechos de acceso, rectificación, supresión, portabilidad, limitación. Puede acceder a la información restante enviando un e-mail a **\*\*\*EMAIL.1***”.

Asimismo, figura el apartado “*Información sobre protección de datos*” en la que figura como responsable la entidad IYANSA QUALITY SL. y describiendo los apartados de: fines, base jurídica, plazo de conservación, destinatarios, derechos, tipo de datos tratados, procesos.

En la web **\*\*\*URL.1** figura un formulario de contacto en el que se solicitan los datos de: asunto y dirección de correo electrónico y una casilla para clicar la aceptación a las condiciones generales y a la política de privacidad. En esta web también figura como responsable IYANSA QUALITY SL.

En fecha 9 de junio de 2020 desde la Inspección de Datos se accede a diversos medios de comunicación on-line:

- En **\*\*\*PERIÓDICO.1** de fecha 25 de mayo de 2020 se informa que FACUA ha denunciado a la página de “XXXXXXXX” por haber dejado accesibles los nombre y cuentas bancarias de los usuarios
- En **\*\*\*PERIÓDICO.2** de fecha 21 de mayo de 2020 se informa que FACUA ha denunciado antes varios organismos a la tienda online de Gobierno Dimisión por incumplimiento de varias normativas de comercio electrónico, haciendo referencia a la LOPDGDD y al RGPD.

Con fecha 11 de junio de 2020 desde la Inspección de Datos se accede a las url's aportadas por FACUA en su denuncia en la que figuraban datos personales y como resultado muestra el siguiente mensaje “*You don't have permission to access this resource*”.

TERCERO: En fecha 15 de junio de 2021, se solicita información a IYANSA QUALITY SL por notificación electrónica, que tuvo “rechazo automático” al no ser recogida por la entidad, motivo por el cual se remitió un nuevo escrito en fecha 17 de julio de 2020. De la respuesta recibida se desprende lo siguiente:

Respecto de la empresa.

- IYANSA QUALITY, S.L. ha modificado su denominación social y domicilio, conservando el CIF, siendo su nueva denominación RESISTENCIA POPULAR, S.L. y su nuevo domicilio **\*\*\*DIRECCIÓN.1**, **\*\*\*LOCALIDAD.1** de Tres Cantos (Madrid).
- RESISTENCIA POPULAR, S.L. tiene suscrito un contrato de prestación de servicios de alojamiento con SERVYTEC NETWORKS, S.L. de fecha 29 de mayo de 2020 (documentos 3, 5 y 6).
- RESISTENCIA POPULAR, S.L. tiene suscrito un contrato de prestación de servicios de mantenimiento de páginas webs con SERVYTEC NETWORKS, S.L. de fecha 29 de mayo de 2020. (documentos 4 y 7)

Respecto de la cronología de los hechos y acciones tomadas.

- Con fecha 19 de junio de 2020 se abre la tienda online de Gobierno Dimisión.
- Con fecha 24 de junio se reciben dos emails de FACUA informando del fallo de seguridad motivo por el cual cierran la tienda online el 25 de junio, descubriendo la brecha el 29 de junio.

Una vez detectado se proceda a realizar una modificación que impide el acceso a las carpetas disponible en la web y se reabre la tienda el 30 de junio.

Respecto de las causas que hicieron posible la brecha.

- RESISTENCIA POPULAR manifiesta el software utilizado (Prestashop- plataforma de eCommerce que permite crear tiendas online) por defecto deja publicar carpetas con archivos temporales en los que se incluyen los archivos que los usuarios cargan a través del formulario de contacto.
- RESISTENCIA POPULAR manifiesta que para solucionarlo modificaron la configuración por defecto del Prestashop desde los archivos raíz para evitar

poder listar las carpetas y se deshabilitó la subida de archivos a través de [\\*\\*\\*URL.18.](#)

- RESISTENCIA POPULAR, S.L. cree que se ha tratado de un error humano de programación por parte del encargado del tratamiento, que no tuvo en cuenta la configuración por defecto de Prestashop y fue fácilmente corregido en cuanto detectaron el fallo.

#### Respecto de los datos afectados.

- RESISTENCIA POPULAR manifiesta que el número de personas afectadas son 6 y los datos corresponden nombre y apellidos.

A este respecto, aporta informe del Delegado de Protección de Datos donde figuran los seis documentos accedidos con datos personales de nombre y apellidos. Estos documentos corresponden con algunos de los aportados por FACUA en su denuncia.

- RESISTENCIA POPULAR manifiesta que no tiene conocimiento de la utilización de terceros de los datos de las personas afectadas y solo tienen constancia del acceso a los datos por el denunciante FACUA.

Asimismo, manifiesta que hechas búsquedas en Internet no aparece el archivo ni datos accedidos de ninguna de las seis personas.

A este respecto, con fecha 18 de enero de 2021 desde la Inspección de Datos se han realizado búsquedas en Google del nombre y apellidos de las seis personas afectadas según RESISTENCIA POPULAR, no encontrando constancia de que los datos existen en Internet sean consecuencia de la brecha.

- RESISTENCIA POPULAR manifiesta que ha notificado la quiebra a las seis personas afectadas y aporta escrito en el que se informa que *“han podido constatar la existencia de una carpeta de archivos temporales (que se elimina cada 7 días) donde se recogían las imágenes enviadas a través del formulario de la web. Es ahí donde hemos podido constatar que usted envió una imagen, siendo su nombre y primer apellido el único dato al que se pudo acceder sin su permiso, destacando que el número total de personas afectadas por el precitado motivo asciende a 6”*.

#### Respecto de las medidas de seguridad implantadas con anterioridad la brecha.

- RESISTENCIA POPULAR informa que las medidas de seguridad son las adoptadas por el encargado del tratamiento haciendo referencia a las que figuran en la web [\\*\\*\\*URL.19](#) y [\\*\\*\\*URL.20](#).

#### Respecto de las medidas implementadas con posterioridad la brecha.

- RESISTENCIA POPULAR ha aportado documento *“Informe de Auditoria. Registro de Actividades de tratamiento de datos personales”* actualizado a fecha 6 de julio de 2020 (documento 8) en el que figura:
  - o Registro de actividades de tratamiento.
  - o Encargados de tratamiento y modelo de encargado y subencargado.
  - o Modelos de ejercicio de derechos.

o Medidas de seguridad: Gestión de usuarios, copias de seguridad, cookies, medidas organizativas, formación, gestión de brechas

Respecto del motivo por el cual no se ha notificado la brecha a la AEPD.

- RESISTENCIA POPULAR manifiesta que no ha notificado como brecha de seguridad el incidente tras haber realizado el estudio previo de las circunstancias que acompañan a lo sucedido y haber concluido que no es una violación de seguridad notificable, por entender que no se considera un alto riesgo para los derechos y libertades de las seis personas afectadas.

CUARTO: En fecha 26 de febrero de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por presunta infracción del artículo 32 del RGPD, artículo 5.1.f) del RGPD, artículo 13 del RGPD, tipificada en el Artículo 83.5 del RGPD.

QUINTO: En fecha 8 de abril de 2021, se formuló propuesta de resolución, en la que se proponía,

<<Que por la Directora de la Agencia Española de Protección de Datos se imponga a IYANSA QUALITY, S.L. con CIF B67580696, una sanción de apercibimiento, por infracción del artículo 5.1.f), en relación con el artículo 5 de la LOPDGDD, conforme lo dispuesto en el artículo 83.5 del RGPD, considerada muy grave a efectos de prescripción en el artículo 72, apartado 1. i) de la LOPDGDD, por infracción del artículo 13 conforme a lo dispuesto en el artículo 83.5, calificada como muy grave a efectos de prescripción en el artículo 72 apartado 1 h) y por infracción del artículo 32 del RGPD conforme a lo dispuesto en el artículo 83.4 del citado RGPD, calificada como grave a efectos de prescripción en el artículo 73 apartado f) de la LOPDGDD. >>

SEXTO: La entidad reclamada no ha presentado alegaciones a la Propuesta de Resolución. \_

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: Se presenta reclamación por el presunto incumplimiento de la normativa de protección de datos en el sitio web [\\*\\*\\*URL.3](#) y [\\*\\*\\*URL.1](#) al considerar que no se estaría proporcionando al usuario información clara y completa sobre el tratamiento de datos personales. En otras denuncias, FACUA manifiesta que han comprobado que en la misma plataforma se tienen archivados toda una serie de documentos en los que se recogen datos personales de terceros sin ninguna clase de medida de protección y accesible por terceros.

SEGUNDO: Consta que en fecha 24 de junio se informa del fallo de seguridad, motivo por el cual cerraron la tienda on line al día siguiente, descubriendo la brecha de seguridad el 29 de junio.

TERCERO: La incidencia tiene su origen en un error de programación. El número de personas afectadas son 6 y los datos corresponden a nombre y apellidos.

## FUNDAMENTOS DE DERECHO

### I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los arts. 47 y 48.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

### II

El artículo 5.1.f) del RGPD, Principios relativos al tratamiento, señala 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»).*

En el presente caso, la brecha de seguridad debe ser calificada de confidencialidad como consecuencia del acceso no autorizado o ilícito a datos personales por terceros ajenos.

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”.*

En el presente caso, consta acreditado que datos personales de usuarios fueron indebidamente expuestos a terceros, vulnerando el principio de confidencialidad establecido en el citado artículo 5.1.f) del RGPD.

### III

El artículo 13 del RGPD, establece la información que se debe proporcionar al interesado en el momento de recogida de sus datos personales:

*“1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:*

*a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;*



- b) los datos de contacto del delegado de protección de datos, en su caso;
- c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
- d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
- e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
- f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

*2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:*

- a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;*
- b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;*
- c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;*
- d) el derecho a presentar una reclamación ante una autoridad de control;*
- e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;*
- f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.*



Por parte de esta Agencia, se ha comprobado que en la web denunciada existe un formulario de contacto en el que se solicitan los datos de: nombre, email, teléfono y mensaje con la siguiente cláusula: “El RESPONSABLE del tratamiento es IYANSA QUALITY SL domicilio en C/ **\*\*\*DIRECCIÓN.2**, BARCELONA. Fines: gestión de la solicitud, registro, compra o consulta. Puede ejercer los derechos de acceso, rectificación, supresión, portabilidad, limitación. Puede acceder a la información restante enviando un e-mail a [\\*\\*\\*EMAIL.1](mailto:***EMAIL.1)”.

La recogida de datos de carácter personal a través de formularios incluidos en una página web constituye un tratamiento de datos, respecto del cual el responsable del tratamiento ha de dar cumplimiento a lo previsto en el artículo 13 del RGPD. En este supuesto, se ha constatado que el sitio web no proporciona al usuario una información clara y completa sobre el tratamiento de sus datos personales.

#### IV

En cuanto a la seguridad de los datos personales, el artículo 32 del RGPD “Seguridad del tratamiento”, establece que:

*“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”.*

## V

El RGPD define las violaciones de seguridad de los datos personales 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”*.

IYANSA QUALITY, SL ha vulnerado el artículo 32 del RGPD, al producirse una brecha de seguridad en sus sistemas como consecuencia de un fallo de seguridad permitiendo potencialmente que cualquiera acceda a a documentos con datos personales.

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”*.

La responsabilidad de IYANSA QUALITY, S.L. viene determinada por la quiebra de seguridad puesta de manifiesto por el reclamante, 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 y, entre ellas, las dirigidas a restaurar la

disponibilidad y el acceso a los datos de forma rápida en caso de incidente físico o técnico. Sin embargo, de la documentación aportada se desprende que la entidad incumplió esta obligación, por cuanto los procedimientos implantados no impidieron que terceros pudieran tener la posibilidad de acceder a datos que les son ajenos.

## VI

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.*

Establece el artículo 72 de la LOPDGDD, bajo la rúbrica de infracciones consideradas muy graves, 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.”*

Por su parte, el artículo 72.1.h) de la LOPDGDD, considera muy grave, a efectos de prescripción, *“la omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del RGPD”*

Establece el artículo 73 de la LOPDGDD, bajo la rúbrica “Infracciones consideradas graves”, lo siguiente:

*“1. 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.*

La vulneración del principio de confidencialidad (art 5.1.f) RGPD) junto a la ausencia de medidas de seguridad (art 32 RGPD) adecuadas en función del riesgo, constituyen el elemento de la culpabilidad que requiere la imposición de sanción.

En el presente caso concurren las circunstancias previstas en los artículos 83.5 y 83.4 del RGPD y 72.1 i) y h) y 73 f) de la LOPDGDD arriba transcritos.

## VII

El artículo 58.2 del RGPD, señala lo siguiente:

*2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:*

*(...)*

- a) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;*

## VIII

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:*

- b) Los responsables de los tratamientos.”*

De lo anterior consta, que la entidad investigada ha infringido el artículo 5.1.f), en relación con el artículo 5 de la LOPDGDD, conforme lo dispuesto en el artículo 83.5 del RGPD, considerada muy grave a efectos de prescripción en el artículo 72, apartado 1. i) de la LOPDGDD, el artículo 13 conforme a lo dispuesto en el artículo 83.5, calificada como muy grave a efectos de prescripción en el artículo 72 apartado 1 h) y el artículo 32 del RGPD conforme a lo dispuesto en el artículo 83.4 del citado RGPD, calificada como grave a efectos de prescripción en el artículo 73 apartado f) de la LOPDGDD.

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 **IYANSA QUALITY SL**, con CIF B67580696, por una infracción del Artículo 32 del RGPD, Artículo 5.1.f) del RGPD, Artículo 13 del RGPD, tipificada en el Artículo 83.5 del RGPD, una sanción de apercibimiento.

SEGUNDO: NOTIFICAR la presente resolución a **IYANSA QUALITY SL**.

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.

938-131120

Mar España Martí

Directora de la Agencia Española de Protección de Datos