- **Expediente Nº: PS/00493/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Dª. ***A.A.A.*** y D. ***B.B.B.*** (en adelante, las partes RECLAMANTES) con fecha 21 de abril de 2021 interpusieron reclamación ante la AEPD. La reclamación se dirige contra D. ***C.C.C.*** con NIF ******NIF.1*** (en adelante, la parte RECLAMADA).

Los motivos en que basa la reclamación son los siguientes:

Las partes RECLAMANTES manifiestan que se ha producido una brecha de seguridad causada por la remisión de un correo electrónico sin copia oculta por la parte RECLAMADA, siendo su contenido accesible a terceros.

Las partes RECLAMANTES manifiestan que no tienen relación con los otros destinatarios del correo electrónico.

Al margen de las direcciones de correo electrónico y de la controversia existente, se revelan los nombres y apellidos de los afectados, así como la dirección en la que se encuentra ubicada su vivienda en construcción.

Junto a la reclamación se aporta copia del mensaje enviado por el reclamado, de fecha 29 de diciembre de 2020.

SEGUNDO: A la vista de los hechos denunciados en la reclamación y de los documentos aportados por el reclamante, 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.

La notificación del traslado de la reclamación se llevó a cabo, vía postal en el domicilio conocido del reclamado, resultando devuelto este envío por el Servicio de Correos con la indicación "Desconocido".

TERCERO: En fecha 6 de agosto de 2021, y de conformidad con lo dispuesto en el art. 65.5 de la LOPDGDD se produjo la admisión a trámite de la reclamación interpuesta por las partes RECLAMANTES.

CUARTO: En fecha 10 de septiembre de 2021 y en respuesta a la solicitud de información remitida por la Subdirección General de Inspección de Datos, tiene entrada en esta Agencia escrito del reclamado en el que manifiesta lo siguiente:

- El envío del correo electrónico el día 29 de diciembre de 2020 a varios destinatarios ha sido intencionado para informar a los destinatarios de la resolución del contrato de la obra contratada con los reclamantes.
- Manifiesta que todos los destinatarios están relacionados, siendo el propio reclamado el nexo de unión.
- En el mismo escrito de respuesta enumera a los destinatarios del correo y la relación existente con cada uno, identificando al menos a nueve de ellos como propietarios de otras obras en las que presta sus servicios y que, según manifiesta, comparten arquitecto y/o instalador eléctrico.
- Aporta copia del Registro de Actividades del Tratamiento de Clientes Potenciales, tratamiento en el que circunscribe el envío del correo electrónico.
- Declara que no ha considerado que el envío realizado constituía una brecha de seguridad; y por este motivo no ha llevado a cabo los requerimientos que establece el RGPD respecto a las brechas de seguridad en sus artículos 33 y 34.
- Manifiesta que ha cambiado el procedimiento de envío de correo cuando van dirigidos a múltiples destinatarios consistente en utilizar la opción que ofrece la aplicación de correo electrónico a través del campo conocido como «copia oculta» (CCO) y que ha recibido formación sobre los riesgos de utilizar el correo electrónico, se ha documentado con las herramientas publicadas por INCIBE (por ejemplo, en su blog se trata este tema “CCO, el (todavía) gran desconocido” o “Decálogo de medidas de seguridad en el correo electrónico”
- Considera oportuno que se tenga en consideración las siguientes circunstancias:

  a) El carácter aislado de la posible infracción.
  b) No se trata de un envío masivo a potenciales y clientes.
  c) El reconocimiento de los hechos, sin intencionalidad alguna (dolo) y la falta de reincidencia.
  d) No realiza envíos de correos electrónicos ni siquiera con fines promocionales o publicitarios de su actividad o servicios (ausencia de finalidad de marketing)
  e) La vinculación de su actividad con la realización de tratamientos de datos personales.
  f) La nulidad de beneficios obtenidos como consecuencia de la comisión de la posible infracción, que solo se realizó a efectos de transparencia con las partes implicadas.
  g) La no afectación a los derechos de menores ni el tratamiento de datos de categorías especiales (tan solo direcciones de correo electrónico).
  h) Se trata de un profesional autónomo.

QUINTO: En fecha 22 de diciembre de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la entidad reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en

adelante, LPACAP), por la presunta infracción de los artículos 5.1.f) y 32 del RGPD, tipificadas en los artículos 83.5 y 83.4 del RGPD.

SEXTO: Notificado el citado acuerdo de inicio, la parte reclamada presentó escrito de alegaciones en el que, en síntesis, se ratifica en lo expuesto en su anterior escrito presentado el pasado 10 de septiembre de 2021 y manifiesta que reconoce expresamente que se han infringido los preceptos legales establecidos, por no utilizar la opción que ofrece la aplicación de correo electrónico a través del campo conocido como «copia oculta» (CCO), para poder realizar un envío sin que se muestren las direcciones de correo de todos ellos; si bien, es cierto que se hizo sin ningún ánimo de ocasionar ningún daño a los destinatarios del correo electrónico.

El envío del correo electrónico el día 29 de diciembre de 2020 a varios destinatarios, aunque fue realizado intencionadamente para informar a dichos destinatarios de la resolución del contrato de obra contratada con la parte RECLAMANTE, en ningún momento influiría en su condición de director de ejecución de sus obras, actuando con la más estricta profesionalidad pese a que el instalador eléctrico de dichas obras fuera el ahora RECLAMANTE, dando el visto bueno a sus trabajos si cumplía correctamente con su cometido, con independencia de las controversias surgidas en su obra de la C/ Almendros 18.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

## HECHOS

PRIMERO: El día 29 de diciembre de 2020 se envió correo electrónico sin copia oculta por la parte RECLAMADA, siendo su contenido accesible a terceros.

SEGUNDO: La parte RECLAMADA reconoce expresamente que se han infringido los preceptos legales establecidos, por no utilizar la opción que ofrece la aplicación de correo electrónico a través del campo conocido como «copia oculta» (CCO), para poder realizar un envío sin que se muestren las direcciones de correo de todos ellos.

Se manifiesta por la parte RECLAMADA que ha cambiado el procedimiento de envío de correo cuando van dirigidos a múltiples destinatarios consistente en utilizar la opción que ofrece la aplicación de correo electrónico a través del campo conocido como «copia oculta» (CCO) y que ha recibido formación sobre los riesgos de utilizar el correo electrónico, se ha documentado con las herramientas publicadas por INCIBE (por ejemplo, en su blog se trata este tema “CCO, el (todavía) gran desconocido” o “Decálogo de medidas de seguridad en el correo electrónico”.

## FUNDAMENTOS DE DERECHO

### I

De acuerdo con los poderes que el artículo 58.2 del (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*."

II

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas establece en relación con la terminación en los procedimientos sancionadores que:
*"Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda".*

III

De conformidad con las evidencias de las que se dispone en el presente momento del procedimiento sancionador, se considera que los hechos probados son constitutivos de infracción.
Se imputa a la parte reclamada la comisión de una infracción por vulneración del Artículo 5.1.f) del RGPD, que señala que:
"*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 transcripción*".
La infracción se tipifica en el Artículo 83.5.a) del RGPD, que considera como tal:
*"los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9"*.

IV

Esta infracción puede ser sancionada con multa de 20.000.000 € 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, de acuerdo con el artículo 83.5 del RGPD.

V

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:
*2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:*

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

VI

De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción por infracción del artículo 5.1 f) a la parte reclamada, como responsable de la citada infracción tipificada en el artículo 83.5 del RGPD, y estimadas las alegaciones presentadas por la parte reclamada, por las circunstancias del caso, procede graduar la multa teniendo en consideración las siguientes atenuantes:
. La escasa vinculación de la actividad profesional desarrollada con el tratamiento de los datos de carácter personal.
. Medidas tomadas para evitar futuros daños y perjuicios: modificación del procedimiento de envío de correo cuando van dirigidos a múltiples destinatarios consistente en utilizar la opción que ofrece la aplicación de correo electrónico a través del campo conocido como «copia oculta» (CCO) y la recepción de formación sobre los riesgos de utilizar el correo electrónico, documentándose con las herramientas publicadas por INCIBE (por ejemplo, en su blog se trata este tema "CCO, el (todavía) gran desconocido" o "Decálogo de medidas de seguridad en el correo electrónico".

Considerando los factores expuestos, procede dirigir un APERCIBIMIENTO por infracción del artículo 5.1 f) del RGPD.

VII

De conformidad con las evidencias de las que se dispone en el presente momento del procedimiento sancionador, se considera que los hechos probados son constitutivos de infracción.
Se imputa a la parte reclamada la comisión de una infracción por vulneración del Artículo 32 del RGPD, que señala 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".*

VIII

Esta infracción puede ser sancionada con multa de 10.000.000 € 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, de acuerdo con el artículo 83.4 del RGPD.

IX

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

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

X

De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción por infracción del artículo 32 del RGPD a la parte reclamada, como responsable de la citada infracción tipificada en el artículo 83.4 del RGPD, y estimadas las alegaciones presentadas por la parte reclamada, por las circunstancias del caso, procede graduar la multa teniendo en consideración las siguientes atenuantes:
. La escasa vinculación de la actividad profesional desarrollada con el tratamiento de los datos de carácter personal.
. Medidas tomadas para evitar futuros daños y perjuicios: modificación del procedimiento de envío de correo cuando van dirigidos a múltiples destinatarios consistente en utilizar la opción que ofrece la aplicación de correo electrónico a través del campo conocido como «copia oculta» (CCO) y la recepción de formación sobre los riesgos de utilizar el correo electrónico, documentándose con las herramientas publicadas por INCIBE (por ejemplo, en su blog se trata este tema "CCO, el (todavía) gran desconocido" o "Decálogo de medidas de seguridad en el correo electrónico".

Considerando los factores expuestos, procede dirigir un APERCIBIMIENTO por infracción del artículo 32 del RGPD.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DIRIGIR APERCIBIMIENTO a D. ***C.C.C.*** con NIF ******NIF.1***, por las infracciones de los artículos 5.1.f) y 32 del RGPD, tipificadas en los artículos 83.5 y 83.4 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a Dª***. A.A.A.*** y D. ***B.B.B.***.

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