- **Expediente Nº: EXP202204552**

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 5 de julio de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***WALL BOX CHARGERS S.L.*** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202204552
IMI Reference: A56ID 388822

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.*** (en adelante, la parte reclamante) con fecha 28 de enero de 2022 interpuso reclamación ante la autoridad irlandesa de protección de datos. La reclamación se dirige contra WALL BOX CHARGERS S.L. con NIF B66542903 (en adelante, WALLBOX). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante ha recibido varios correos de otros clientes de WALLBOX debido a que un empleado de WALLBOX le puesto en copia (CC) de correos a otros clientes, y está recibiendo las contestaciones a ese correo inicial. Por este motivo, la parte reclamante ha recibido datos (nombre y dirección de correo electrónico) de, al menos, otros 4 clientes de WALLBOX. Después de esto, la parte reclamante se puso en contacto con WALLBOX y con el empleado de WALLBOX que le había puesto en copia de sus emails. Y recibió una respuesta del empleado de WALLBOX indicando que esto era una cosa sin importancia y ofreciéndole un descuento del 10% por las molestias ocasionadas.

Junto con la reclamación se aporta:

- Impresión de un correo electrónico enviado desde la dirección ******USUARIO.1**@*wallbox.com* a ******USUARIO.2@gmail.com,**** el 27 de enero de 2022 a las 16:41hs, con el siguiente texto:
"Dear EV - Enthusiast,
thank you for your interest in our wallbox chargers.
You reached out to us a few weeks ago because you have questions about our products or you need
consulting in general?
If you have questions, please feel free to reach out to me.
I can also offer to call you.
P.S.: With the code: (...) you get a 5% discount on every charger in our Online Shop.
Kind regards"

[Traducción no oficial: "*Estimado EV- Entusiasta, gracias por tu interés en nuestros cargadores wallbox.*
¿Nos contactaste hace unas semanas porque tenías preguntas sobre nuestros productos o necesitas una asesoría general?
Si tienes preguntas, por favor siéntete libre de contactarme.
También te ofrezco llamarte. (…)"]

- Impresión de un correo electrónico enviado en respuesta al anterior desde la dirección ******USUARIO.2@gmail.com*** a ******USUARIO.1****@wallbox.com, el 27 de enero de 2022 a las 16:41hs, con el siguiente texto:

"*After receiving your reply earlier today I have been receiving emails from OTHER WALLBOX CUSTOMERS. These customers have been trying to reply to Wallbox (i.e. you), but you CC'd me in your replies and now I am the one receiving responses. You have breached data protection laws and have exposed the personal data of multiple customers including myself. If I was a nefarious person I could have easily exploited this situation to scam or obtain further personal information from other customers including possibly tricking them into sending me money as they think they are contacting Wallbox support.*

So far I have received emails from:

B.B.B. - ******USUARIO.3@gmail.com***
C.C.C. - ******USUARIO.4@practiceevolve.com***
D.D.D.- ******USUARIO.5@gmail.com***
E.E.E.- ******USUARIO.6@emmotorsport.com***

This is complete negligence on your behalf and you have put the personal information of multiple customers at risk. I will be reporting this to the Data Protection Commission of Ireland. I will also be emailing each of those customers individually to let them know that their information has potentially been compromised. And I would also like this to be escalated to an official complaint with Wallbox as this situation is ridiculous. No doubt you have probably CC'd me in other customers emails also, and I expect that I am going to receive more emails over the coming days from them."

[Traducción no oficial:
"Después de recibir su respuesta el día de hoy he estado recibiendo correos electrónicos de OTROS CLIENTES DE WALLBOX. Estos clientes han estado tratando

de responder a Wallbox (es decir, usted), pero usted me hizo CC en sus respuestas y ahora yo soy el que recibe respuestas. Usted ha infringido las leyes de protección de datos y ha expuesto los datos personales de múltiples clientes, incluido yo mismo. Si yo fuera una persona nefasta, podría haber explotado fácilmente esta situación para estafar u obtener más información personal de otros clientes, incluyendo posiblemente engañarlos para que me envíen dinero, ya que creen que están contactando con el soporte de Wallbox.

Hasta ahora he recibido correos electrónicos de:

B.B.B. *-* ******USUARIO.3@gmail.com***
C.C.C. *-* ******USUARIO.4@practiceevolve.com.au***
D.D.D.*-* ******USUARIO.5@gmail.com***
E.E.E.*-* ******USUARIO.6@emmotorsport.com***

Esto es una total negligencia por su parte y ha puesto en riesgo la información personal de múltiples clientes. Informaré de esto a la Comisión de Protección de Datos de Irlanda. También enviaré un correo electrónico a cada uno de esos clientes individualmente para hacerles saber que su información ha sido potencialmente comprometida. Y también me gustaría que esto se elevara a una queja oficial con Wallbox, ya que esta situación es ridícula. Sin duda usted probablemente me ha puesto en copia en otros correos electrónicos de clientes, y espero recibir más correos electrónicos en los próximos días de ellos."]

- Impresión de un correo electrónico enviado en respuesta al anterior desde la dirección ******USUARIO.1****@wallbox.com* a ******USUARIO.2@gmail.com****,* el 28 de enero de 2022 a las 11:28hs, con el siguiente texto:

"*I am so sorry for the inconveniences. This was not intentional.*
I used the <<BCC>> functionality:
BCC, which stands for blind carbon copy, allows you to hide recipients in email messages. Addresses in the To: field and the CC: (carbon copy) field appear in messages, but users cannot see addresses of anyone you included in the BCC: field.
But in any case you dont need to worry at all, it was just a reminder email to people like yourself to offer help regarding a wallbox. So nothing bad and nothing will happen.
I can only repeat myself: I am sorry, i dont understand how this is possible, honestly. I want to offer you a discount for a wallbox as a compensation: 10% with the code: ***(…)***"

[Traducción no oficial:
"Lo siento mucho por los inconvenientes. Esto no fue intencionado.
Utilicé la funcionalidad <<BCC>>:
BCC, que significa copia de carbono ciega, le permite ocultar a los destinatarios en los mensajes de correo electrónico. Las direcciones en el campo Para: y el campo CC: (copia de carbono) aparecen en los mensajes, pero los usuarios no pueden ver las direcciones de nadie que haya incluido en el campo BCC:.
Pero en cualquier caso no necesita preocuparse en absoluto, era solo un correo electrónico de recordatorio a personas como usted para ofrecer ayuda con respecto a una wallbox. Así que nada malo sucede ni sucederá.
Solo puedo repetirme: Lo siento, no entiendo cómo ha pasado, honestamente. Quiero ofrecerle un descuento para una wallbox como compensación: 10 % con el código: ***(…)****"]*

- Impresión de un correo electrónico enviado en respuesta al anterior desde la dirección ******USUARIO.1****@wallbox.com a ******USUARIO.2@gmail.com****, el 28 de enero de 2022 a las 13:40hs, con el siguiente texto:

"*Whether it was intentional or not this is a data breach and you have a responsibility to your company and to your customers to report it. If it was an error with your IT systems rather than human error then it should be reported to your IT department to investigate the cause and implement a fix to prevent it from happening again. What exactly are you and your company doing to investigate this and what remedial actions are you taking to prevent this from re-occuring? As i said in my previous email i would like this to be raised as an OFFICIAL COMPLAINT with Wallbox.*
The fact that you are brushing this off as "nothing bad" is not very comforting and I don't think you understand the risk to customers that exists with that attitude. And is an especially bad attitude from a company that deals with the day to day collection of customer data from the Wallbox app. Whether you use CC or BCC is irrelevant as I now have the NAMES and PERSONAL email addresses of four other Wallbox customers which I should NEVER have access to and they also have access to my own name and personal email which additionally put myself at risk.
As I explained in my previous email, under different circumstances this situation could have been exploited to get further personal information or even be used to defraud customers by posing as Wallbox Support. I work in an organisation that deals with cyber security issues just like this and I know for a fact that that kind of risk is very real."

[Traducción no oficial:
"Independientemente de si fue intencionado o no, esto es una violación de datos y usted tiene la responsabilidad con su empresa y con sus clientes de informarlo. Si fue un error con sus sistemas de TI en lugar de un error humano, entonces debe informarse a su departamento de TI para investigar la causa e implementar una solución para evitar que vuelva a suceder. ¿Qué están haciendo exactamente usted y su compañía para investigar esto y qué medidas correctivas está tomando para evitar que esto vuelva a ocurrir? Como dije en mi correo anterior me gustaría que esto se planteara como una QUEJA OFICIAL a Wallbox.
El hecho de que estés descartando esto como «nada malo» no es muy reconfortante y no creo que entiendas el riesgo para los clientes que existe con esa actitud. Y es una actitud especialmente mala de una empresa que se ocupa de la recopilación diaria de datos de clientes desde la aplicación Wallbox. Ya sea que use CC o BCC es irrelevante, ya que ahora tengo las direcciones de correo electrónico PERSONAL y NOMBRES de otros cuatro clientes de Wallbox a los que nunca debería tener acceso y ellos también tienen acceso a mi propio nombre y correo electrónico personal que, además, me pone en riesgo.
Como expliqué en mi correo electrónico anterior, en diferentes circunstancias esta situación podría haber sido explotada para obtener más información personal o incluso para defraudar a los clientes haciéndose pasar por el servicio de atención al cliente de Wallbox. Trabajo en una organización que se ocupa de problemas de seguridad cibernética como este y sé a ciencia cierta que ese tipo de riesgo es muy real."]

SEGUNDO: A través del "Sistema de Información del Mercado Interior" (en lo sucesivo Sistema IMI), regulado por el Reglamento (UE) nº 1024/2012, del Parlamento Europeo

y del Consejo, de 25 de octubre de 2012 (Reglamento IMI), cuyo objetivo es favorecer la cooperación administrativa transfronteriza, la asistencia mutua entre los Estados miembros y el intercambio de información, se transmitió la citada reclamación el día 13 de abril de 2022 y se le dio fecha de registro de entrada en la Agencia Española de Protección de Datos (AEPD) el día 18 de abril de 2022. El traslado de esta reclamación a la AEPD se realiza de conformidad con lo establecido en el artículo 56 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/2016, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos (en lo sucesivo, RGPD), teniendo en cuenta su carácter transfronterizo y que esta Agencia es competente para actuar como autoridad de control principal, dado que WALLBOX tiene su sede social y establecimiento principal en España.

Los tratamientos de datos que se llevan a cabo afectan a interesados en varios Estados miembros. Según las informaciones incorporadas al Sistema IMI, de conformidad con lo establecido en el artículo 60 del RGPD, actúa en calidad de "autoridad de control interesada", además de la autoridad de protección de datos de Irlanda, las autoridades de Suecia, Austria, Países Bajos, Bélgica, Polonia, Francia, Estonia, Italia, Eslovaquia y las autoridades alemanas de Renania-Palatinado y Berlín. Todas ellas en virtud del artículo 4.22 del RGPD, dado que los interesados que residen en el territorio de estas autoridades de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento objeto del presente procedimiento.

TERCERO: Con fecha 8 de junio de 2022, de conformidad con el entonces vigente artículo 64.3 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: El 16 de noviembre de 2022 la AEPD solicita, a través del Sistema IMI, a la autoridad de protección de datos de Irlanda que la parte reclamante aporte los correos electrónicos originales que se enviaron a los otros clientes y a él también (los correos electrónicos que dieron lugar a esta reclamación).

La autoridad de protección de datos de Irlanda compartió a través de IMI, el día 9 de enero de 2023 la documentación solicitada.

QUINTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del RGPD, y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

El día 5 de diciembre de 2022, se presenta un escrito ante la AEPD en nombre de WALLBOX como respuesta a requerimiento de información (este requerimiento de información fue accedido por WALLBOX el 21 de noviembre de 2022), con número de registro de entrada ******REGISTRO.1***, en el que se aporta, entre otra, la siguiente información:

1. Declaración de que las causas del incidente descrito por la parte reclamante "*se trata de error humano en el uso de la funcionalidad normal del campo BCC (Blind carbon copy o copia oculta) en el envío de correos electrónicos. En este caso concreto, una persona del equipo de pre-venta utilizó los datos de contacto de distintas personas (65) que los habían proporcionado mediante los formularios de más información disponibles en la página web o redes sociales. Se trata de un mensaje de respuesta a una petición de información genérica realizada por los interesados mediante formularios predefinidos y, por tanto, se responden manualmente por parte de nuestro equipo comercial de forma también predefinida. De conformidad con nuestros procedimientos internos, al enviar siempre un primer mensaje estándar, se utiliza la funcionalidad de copia oculta a fin de optimizar las cargas de trabajo y poder enviar múltiples correos en una sola acción, sin desvelar la identidad o correo electrónico de todos los destinatarios. Sin embargo, como decimos, debido a un error humano por parte de la persona que envió ese correo en particular, se incluyó UNA dirección de correo electrónico en el campo CC y no BCC".* Dicha dirección es la de la parte reclamante.

2. Declaración, respecto a los datos afectados de lo siguiente:

   - *64 personas que recibieron el correo pudieron visualizar la dirección de correo* electrónico de la parte reclamante*.*

   - La parte reclamante pudo visualizar la dirección de correo electrónico de aquellos que contestaron al correo enviado por WALLBOX utilizando "responder a todos" y sin eliminar la dirección ******USUARIO.2@gmail.com***, lo que ocurrió en 4 correos. Al ser una respuesta enviada por los interesados, la parte reclamante pudo visualizar igualmente el nombre y apellidos de dichas personas (si incluyeron información veraz al registrarse en los correspondientes servicios de correo electrónico).

3. Declaración, respecto a las posibles consecuencias para los afectados, de que "*viendo la potencial información afectada, consideramos que difícilmente puede haber ninguna real. No se ha filtrado ninguna información relevante más allá de cuentas de correo electrónico (2 cuentas genéricas @gmail.com y 2 que parecerían profesionales) y potencialmente nombres y apellidos, por lo que no consideramos la existencia de consecuencias relevantes, más allá de potenciales suplantaciones de identidad o phishing que bien podrían hacerse igualmente mediante correos electrónicos inventados o aleatorios, en tanto que en ningún momento ninguna de las personas afectadas ha obtenido ningún otro tipo de información que la dirección del correo electrónico.*". De este modo, indican que "*Tal y como puede apreciarse en el informe remitido a esta Agencia, consideramos que el riesgo vinculado al incidente era insuficiente para considerarlo una brecha que debiera ser notificada a la autoridad de control.*"

4. Alegan la aplicación de la "*Guía para la gestión y notificación de brechas de seguridad*" publicada por la AEPD y el ISMS, en colaboración con el Centro Criptológico Nacional e Incibe, que en su apartado 9.3 establece: "*No será necesaria la notificación a la Autoridad de Control cuando el responsable pueda demostrar, de forma fehaciente, que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas*".

5. Respecto a la falta de notificación de la brecha a la AEPD, declaran lo siguiente: "*siguiendo los criterios de los ejemplos ilustrativos incluidos por la AEPD y el ISMS en dicha guía, para la toma de decisiones relacionada con la notificación de brechas de seguridad a la autoridad de control, y que WALLBOX considera razonables y vigentes, cabe concluir que el incidente en cuestión no revestía de suficiente relevancia para ser puesto en conocimiento de la autoridad toda vez que, además, (i) no se trató de un ataque informático, (ii) no fallaron medidas de seguridad implementadas y, (iii), existían medidas de seguridad planificadas e implementadas a lo largo de 2022 que mitigan la posibilidad de que este caso volviera a suceder en un futuro.*"

6. Respecto a la comunicación de la brecha a los afectados, declaran que <<*De la misma forma que en el caso anterior, WALLBOX decidió no comunicar el incidente a las personas afectadas por considerar que no era un incidente especialmente relevante para la privacidad de los interesados ni ponía en riesgo sus libertades y derechos de ninguna forma. Asimismo, cabe tener en cuenta que utilizando la herramienta Comunica-Brecha RGPD de la propia AEPD, el resultado que vierte la misma es "No sería necesario comunicar la brecha de seguridad a los afectados", lo que resulta consistente con la valoración del riesgo realizada por WALLBOX, y razón por la que no se comunicó nada a las personas afectadas.*>>

7. Indicación de que antes del incidente se habían aplicado las siguientes medidas de seguridad:

"(...)"

8. Indicación de que, a raíz del presente caso, se han implementado las siguientes mejoras:

"(...)"

9. Copia de informe de este incidente de seguridad que incluye, entre otros apartados, los siguientes:

   - el "*Análisis de riesgos para los derechos y libertades de los interesados*" y el "*Análisis de riesgos para el derecho a la protección de datos*", con el resultado de que el riesgo el BAJO.
   - las medidas de seguridad que se aplicaban antes del incidente
   - las medidas de seguridad aplicadas después del incidente.
   - las evaluaciones de la necesidad de notificar el incidente a la AEPD, donde se aprecia la utilización de la valoración que se describe en la "Guía para la gestión y notificación de brechas de seguridad" publicada por la AEPD, obteniendo una puntuación de 6 puntos y una circunstancia cualitativa, lo cual indican que no es condición suficiente para notificar la brecha a la AEPD ni para comunicar la brecha a los afectados.
   - la "*Evaluación de la necesidad de comunicación a los interesados*", donde se indica que se han seguido los criterios de la herramienta online de la AEPD "Comunica-Brecha RGPD", obteniendo que "*No existe necesidad de comunicar la violación de la seguridad a los interesados*".

CONCLUSIONES

1. La parte reclamante recibió un correo que estaba dirigidos a 64 clientes de WALLBOX. El resto de clientes estaban en copia oculta, por lo que no podía ver sus correos electrónicos. Esto ha llevado al conocimiento de los siguientes datos personales por parte de los clientes de WALLBOX:
   - Si uno de esos 64 clientes contestaba a todos los destinatarios del correo, la parte reclamante recibía un correo de ese cliente en el que aparecía como remitente el correo electrónico de ese cliente y el pseudónimo de ese correo electrónico (que, en muchos casos, coincide con el nombre y apellido del propietario del correo electrónico). Según declaraciones de la parte reclamante, esto ocurrió con 4 clientes.
   - Los 64 clientes a los que estaba dirigido el correo recibieron dentro del correo (en el dato "CC" de la cabecera del correo) la dirección de correo electrónico de la parte reclamante y su pseudónimo.

2. La parte reclamante indica que ha comunicado a los 4 clientes de los que ha recibido correo electrónico que se ha producido esta situación.

3. WALLBOX ha realizado una evaluación de la necesidad de notificación de la brecha a la AEPD y de la necesidad de la comunicación de la brecha a los afectados siguiendo la antigua "Guía para la gestión y notificación de brechas de seguridad" de 2018 elaborada por la AEPD e ISMS Forum Spain. WALLBOX aporta la evidencia de que ha realizado esta evaluación siguiendo el anexo III de esta guía, y obteniendo como resultado que no era necesaria ni la notificación a la AEPD ni la comunicación a los afectados.

SEXTO: De acuerdo con el informe recogido de la herramienta AXESOR el día 13 de abril de 2023, WALLBOX es una empresa de tipo "Filial de grupo" con un volumen de negocio en el año 2021 de 77.079.844 € y 542 empleados.

SÉPTIMO: Con fecha 31 de mayo de 2023, la Directora de la AEPD adoptó un proyecto de decisión de inicio de procedimiento sancionador. Siguiendo el proceso establecido en el artículo 60 del RGPD, ese mismo día se transmitió a través del sistema IMI este proyecto de decisión y se les hizo saber a las autoridades interesadas que tenían cuatro semanas desde ese momento para formular objeciones pertinentes y motivadas. El plazo de tramitación del presente procedimiento sancionador quedó suspendido automáticamente durante estas cuatro semanas, de acuerdo con lo dispuesto en el artículo 64.5 de la LOPDGDD.

Dentro del plazo a tal efecto, las autoridades de control interesadas no presentaron objeciones pertinentes y motivadas al respecto, por lo que se considera que todas las autoridades están de acuerdo con dicho proyecto de decisión y están vinculadas por este, de conformidad con lo dispuesto en el apartado 6 del artículo 60 del RGPD.

FUNDAMENTOS DE DERECHO

I

Competencia y normativa aplicable

De acuerdo con lo dispuesto en los artículos 58.2 y 60 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 y 68.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "*Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos*."

II
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 y 4.2 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que WALLBOX realiza la recogida y conservación de, entre otros, los siguientes datos personales de personas físicas: nombre y apellidos y correo electrónico, entre otros tratamientos.

WALLBOX realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD. Además, se trata de un tratamiento transfronterizo, dado que WALLBOX tiene su establecimiento principal en España, si bien presta servicio a otros países de la Unión Europea.

El RGPD dispone, en su artículo 56.1, para los casos de tratamientos transfronterizos, previstos en su artículo 4.23), en relación con la competencia de la autoridad de control principal, que, sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60. En el caso examinado, como se ha expuesto, WALLBOX tiene su establecimiento principal en España, por lo que la Agencia Española de Protección de Datos es la competente para actuar como autoridad de control principal.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "*violaciones de seguridad de los datos personales*" (en adelante, brecha de seguridad) como "*todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*."

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al

haberse enviado un correo electrónico sin haber ocultado el correo electrónico de la parte reclamante.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III
Principio de integridad y confidencialidad

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"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, consta que los datos personales de la parte reclamante, obrantes en la base de datos de WALLBOX, fueron indebidamente expuestos a terceros, al enviar un correo electrónico sin ocultar su dirección. Asimismo, la parte reclamante ha podido acceder a los nombres y apellidos y correos electrónicos de 4 interesados que respondieron el primer mensaje en cuestión utilizando la opción de responder a todos.

Tal como ha quedado acreditado en el expediente, se envió un correo electrónico de forma manual a 65 personas, en respuesta a una petición de información genérica de los interesados, y se incluyó la dirección de correo electrónico de la parte reclamante en el campo CC y no BCC, por lo que ha quedado accesible a esas otras 64 personas. Además, 4 de estas personas respondieron a la parte reclamante, por lo que ésta pudo acceder a sus nombres y apellidos y correos electrónicos.

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

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

De confirmarse, la citada infracción del artículo 5.1.f) del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)"*

A efectos del plazo de prescripción, el artículo 72 "*Infracciones consideradas muy graves*" de la LOPDGDD indica:

"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

> *a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679. (…)"*

V

Propuesta de sanción por la infracción del artículo 5.1.f) del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- 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 (apartado a): por exponer la dirección de correo electrónico de la parte reclamante a otras 64 personas y por haber sido compartidos con la parte reclamante los nombres y apellidos y correos electrónicos de unas 4 personas.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y artículo 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 5.1.f) del RGPD, permite fijar inicialmente una sanción de 5.000 € (cinco mil euros).

VI

Seguridad del tratamiento

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".

En el presente caso, en el momento de producirse la brecha, no se ha acreditado que WALLBOX contara con medidas apropiadas tendentes a evitar el envío de e-mails sin utilizar la funcionalidad CCO ni tampoco se había puesto especial diligencia a la hora de realizar envíos masivos de correos electrónicos.

De conformidad con las evidencias de las que se dispone en este acuerdo de iniciación del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a WALLBOX, por vulneración del artículo 32 del RGPD.

VII

Tipificación de la infracción del artículo 32 del RGPD

De confirmarse, la citada infracción del artículo 32 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"*

A 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. (…)"

VIII
Propuesta de sanción por la infracción del artículo 32 del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- 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 (apartado a): por no contar con las medidas apropiadas para evitar que se envíen correos electrónicos en los que se incluyan direcciones de los destinatarios sin copia oculta, lo que puede ocasionar que el resto de destinatarios accedan a sus datos de contacto y que se puedan compartir más datos de los destinatarios al responder con copia a todos, afectando de forma directa a 5 interesados, al dejar expuestos los datos de contacto de la parte reclamante a otras 64 personas y permitió que la parte reclamante accediera a nombre y apellido y correo electrónico de otras 4 personas, y de forma potencial a todos sus clientes (más de 6000 al mes, según https://www.computing.es/casos-de-exito/wallbox-se-adelanta-a-las-necesidades-de-un-ciudadano-mas-sostenible/).

- Negligencia en la infracción (apartado b): la actuación de WALLBOX ha sido gravemente negligente en tanto, al haber tenido conocimiento de la situación, se le respondió a la parte reclamante que no iba a pasar nada, pero no hay constancia de que a raíz de la respuesta de la parte reclamante se hubiese investigado la brecha en cuestión y se hubiera implementado una solución para evitar que tales situaciones se repitan. De hecho, el informe aportado a esta Agencia ha sido elaborado precisamente a raíz de que se le hubiera efectuado un requerimiento de información, pero no consta que antes de la intervención de esta Agencia la empresa hubiera realizado las acciones tendentes a analizar lo ocurrido ni a adoptar medidas preventivas o de mitigación de los posibles efectos.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 32 del RGPD, permite fijar inicialmente una sanción de 3.000 € (tres mil euros).

IX
Imposición 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, sin perjuicio 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.

Asimismo, las medidas que pudieran adoptarse en la resolución que ponga fin al procedimiento, en relación con las medidas de seguridad, serán de aplicación en todos los países de la Unión Europea en los que opere WALLBOX.

Se advierte que no atender a los requerimientos de este organismo puede 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 **WALL BOX CHARGERS S.L.**, con NIF **B66542903**, por la presunta infracción de los artículos 5.1.f) y 32 del RGPD, tipificadas en el artículo 83.5 y 83.4 del RGPD, respectivamente.

SEGUNDO: NOMBRAR como instructora a ***F.F.F.*** y, como secretaria, a ***G.G.G.***, 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 documentación procedente del IMI que ha dado lugar a las actuaciones previas de investigación, 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 y la documentación procedente del IMI sobre el proyecto de decisión.

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, tipificada en el artículo 83.5 de dicha norma, multa administrativa de cuantía 5.000,00 euros.

- Por la supuesta infracción, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 3.000,00 euros.

QUINTO: NOTIFICAR el presente acuerdo a **WALL BOX CHARGERS S.L.**, con NIF **B66542903**, 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 6.400,00 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 6.400,00 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 4.800,00 euros.

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

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (6.400,00 euros o 4.800,00 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 se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

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

935-290523

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

>>

SEGUNDO**:** En fecha 13 de julio de 2023, la parte reclamada ha procedido al pago de la sanción en la cuantía de **4800 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

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

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II
Terminación del procedimiento

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

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

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

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

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

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

PRIMERO: DECLARAR la terminación del procedimiento **EXP202204552**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a ***WALL BOX CHARGERS S.L.***.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por

el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

936-040822

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