File No: EXP202204552
IMI Reference: A56ID 388822

FINAL DECISION

From the actions carried out by the Spanish Data Protection Agency and on the basis of the following

BACKGROUND

FIRST: [redacted] (hereinafter the complainant) lodged a complaint with the Irish Data Protection Authority on 28 January 2022. The complaint is directed against WALL BOX CHARGERS S.L. with NIF B66542903 (hereinafter WALLBOX). The grounds on which the complaint is based are as follows:

The complainant has received several emails from other customers of WALLBOX because a WALLBOX employee put [redacted] in copy (CC) of emails to other customers and is receiving replies to that initial mail. For this reason, the complainant has received data (name and e-mail address) from at least 4 other customers of WALLBOX. After this, the complainant contacted WALLBOX and the WALLBOX employee who had put [redacted] in copy of the emails. [redacted] received a reply from the WALLBOX employee stating that this was irrelevant and offering [redacted] a discount of 10 % for the inconvenience caused.

The complaint is accompanied by:

— Screenshot of an email sent from the address [redacted] to [redacted] ***on*** 27 January 2022 at 16:41hs, worded as follows:

"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: [redacted] *you get a 5% discount on every charger in our Online Shop.*
Kind regards"

- Screenshot of an email sent in reply to the previous email from [redacted] to [redacted]*wallbox.com* on 27 January 2022 at 16:41hs, worded as follows:

"*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:

[redacted]

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."

- Screenshot of an email sent in reply to the previous one from [redacted]*wallbox.com* to [redacted] on 28 January 2022 at 11:28hs, with the following wording:

"*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: [redacted]"

- Screenshot of an email sent in reply to the previous one from [redacted]*wallbox.com* to [redacted] on 28 January 2022 at 13:40hs, with the following wording:

"*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."

SECOND: Via the 'Internal Market Information System' (hereinafter 'IMI System'), governed by Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 (the IMI Regulation), the purpose of which is to promote cross-border administrative cooperation, mutual assistance between the Member States and the exchange of information, the complaint was forwarded on 13 April 2022 and was registered with the Spanish Data Protection Agency (AEPD) on 18 April 2022. This complaint is forwarded to the AEPD in accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27/04/2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('GDPR'), taking into account its cross-border nature and that the Agency is competent to act as the lead supervisory authority, given that WALLBOX has its registered office and main establishment in Spain.

The processing of data carried out concerns data subjects in several Member States. According to the information contained in the IMI system, in accordance with Article 60 of the GDPR, in addition to the data protection authority of Ireland, the authorities of Sweden, Austria, the Netherlands, Belgium, Poland, France, Estonia, Italy, Slovakia and the German authorities of Rhineland-Palatinate and Berlin act as a 'concerned supervisory authorities'. All of them under Article 4 (22) GDPR, given that data subjects residing in the territory of these supervisory authorities are substantially affected or are likely to be substantially affected by the processing that is the subject of the present proceedings.

THIRD: On 8 June 2022, in accordance with the Article 64 (3) of Spanish Organic Law 3/2018 of 5 December on the protection of personal data and the guarantee of digital rights (LOPDGDD), the complainant's complaint was declared admissible.

FOURTH: On 16 November 2022, the AEPD requests, via the IMI System, the Irish Data Protection Authority to provide the original emails sent to the other customers and also to the complainant (the emails that gave rise to this complaint).

The Irish Data Protection Authority shared the requested documentation via IMI on 9 January 2023.

FIFTH: The General Subdirectorate for Data Inspection carried out preliminary investigations to clarify the facts in question, in accordance with the tasks assigned to the supervisory authorities in Article 57 (1) and the powers conferred on them in Article 58 (1) of the GDPR, and in accordance with Title VII, Chapter I, second section, of the LOPDGDD, and was aware of the following:

On 5 December 2022, a letter was submitted to the AEPD on behalf of WALLBOX in response to a request for information, with entry registration number [redacted], in which the following information is provided, inter alia:

1. Statement that the causes of the incident described by the complainant "*are human error in the use of the normal functionality of the BCC field (Blind carbon copy or hidden copy) in sending emails. In this particular case, one person from the pre-sales team used the contact details of different persons (65) who had provided them using the more information forms available on the website or social media. This is a message replying to a request for generic information made by data subjects using pre-defined forms and is therefore answered manually by our commercial team in a predefined way. In accordance with our internal procedures, when always sending a first standard message, hidden copying functionality is used to optimise workloads and to be able to send multiple emails in a single action, without revealing the identity or email of all recipients. However, as we have said, due to a human error on the part of the person who sent that particular email, ONE email address was included in field CC and not BCC'.* That address is that of the complainant.

2. Statement, with regard to the data concerned, of the following:

   - 64 people who received the email were able to view the complainant's email address.

   The complainant was able to view the email address of those who replied to the mail sent by WALLBOX using 'reply to all' and without deleting the [redacted] address, which happened in 4 emails. As a reply sent by the data subjects, the complainant was also able to view the first and last name of those persons (if they included truthful information when registering with the relevant email services).

3. Statement, with regard to the possible consequences for those affected, that 'in view of *the potential information affected, we consider that there can hardly be any real one. No relevant information has been leaked other than email accounts (2 generic accounts @gmail .com and 2 which would appear professional) and potentially names and surnames, so we do not consider the existence of significant consequences beyond potential identity or phishing supplantations that could also be done by invented or random emails, whereas at no point in time has any of the persons concerned obtained any information other than the email address.*" Thus, they state that '*As can be seen in the report sent to this Agency, we consider that the risk linked to the incident was insufficient to consider it a breach that should be notified to the supervisory authority.*'

4. They allege the application of the '*Guide to the management and reporting of security breaches*' published by the AEPD, in collaboration with the Spanish National Cybersecurity Institute , which states in paragraph 9.3: "*Notification to the Supervisory Authority shall not be required where the controller can demonstrate in a reliable manner that the personal data security breach does not pose a risk to the rights and freedoms of natural persons*."

5. With regard to the lack of reporting of the breach to the AEPD, they state the following: '*following the criteria in the illustrative examples included by the AEPD in that guide, for decision-making related to the notification of security breaches to the supervisory authority, and which WALLBOX considers reasonable and effective, it can be concluded that the incident in question was not of sufficient relevance to be brought to the attention of the authority, since (i) it was not a computer attack, (ii) no security measures implemented were missing and (iii) there were security measures planned*

and implemented in the course of 2022 to mitigate the possibility that this case might happen again in the future.'

6. With regard to the communication of the breach to those affected, they state that, in *the same way as in the previous case, WALLBOX decided not to communicate the incident to the data subjects because it considered that it was not a particularly relevant incident for the privacy of the data subjects and did not jeopardise their freedoms and rights in any way. It should also be borne in mind that using the AEPD's own GDPR communication tool, the result of this tool is 'It would not be necessary to communicate the security breach to those affected', which is consistent with WALLBOX's risk assessment, and that is why nothing was communicated to the data subjects.>*

7. Indication that the following security measures had been implemented prior to the incident:

[redacted]

8. Indication that, as a result of the present case, the following improvements have been implemented:

[redacted]

9. A copy of the report of this security incident which includes, inter alia, the following:

— the '*Analysis of risks to the rights and freedoms of data subjects*' and the '*Analysis of risks to the right to data protection*', with the result that the risk is LOW.
— the security measures that were in place prior to the incident
— the security measures applied after the incident.
— the assessments of the need to report the incident to the AEPD, which assess the use of the assessment described in the 'Guidance on the management and

reporting of security breach' published by the AEPD, obtaining a score of 6 points and a qualitative circumstance, indicating that this is not a sufficient condition for reporting the breach to the AEPD or for communicating the breach to those affected.

— the '*Assessment of the need for communication to data subjects*', which states that the criteria of the AEPD online tool 'Communication-GDPR' have been followed, finding that '*there is no need to communicate the security breach to data subjects*'.

CONCLUSIONS

1. The complainant received an email addressed to 64 customers of WALLBOX. The other customers were in hidden copy and therefore could not see their emails. This has led to the following personal data being brought to the attention of WALLBOX's clients:
   — If one of those 64 customers replied to all the addressees of the mail, the complainant received an email from that customer showing as the sender the email of that customer and the pseudonym of that email (which, in many cases, coincides with the first name and surname of the owner of the email). According to the complainant, this was the case for 4 customers.
   — The 64 customers to whom the mail was addressed received in the mail (in the 'CC' data on the head of the mail) the email address of the complainant and [redacted] pseudonym.

2. The complainant indicates that [redacted] has informed the 4 customers from whom [redacted] has received e-mail that this situation has occurred.

3. WALLBOX has carried out an assessment of the need to report the breach to the AEPD and of the need to communicate the breach to those affected following the 2018 AEPD previous 'Security Breach Management and Reporting Guide'. WALLBOX has provided evidence that it has carried out this assessment in accordance with Annex III to this guide. As a result, neither notification to the AEPD nor communication to those affected was necessary.

SIXTH: According to the report collected from the AXESOR tool on 13 April 2023, WALLBOX is a 'Group Subsidiary' company with a sales volume in 2021 of 77.079.844 EUR and 542 employees.

SEVENTH: On 5 July 2023 the Director of the Spanish Data Protection Agency decided to initiate penalty proceedings against WALLBOX in order to impose a fine of 5,000 EUR and 3,000 EUR, in accordance with Articles 63 and 64 of the Spanish LPACAP, for the alleged infringement of Article 5 (1) (f) and Article 32 of the GDPR, as defined in Article 83 (5) and 83 (4) of the GDPR, in which it was informed that it had a period of ten days to submit allegations.

This agreement, which was notified in accordance with the rules laid down in the LPACAP by electronic notification, was collected by WALLBOX on 5 July 2023, in accordance with the Spanish Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations (LPACAP), as stated in the acknowledgement of receipt contained in the file.

EIGHTH: On 13 July 2023, WALLBOX paid the penalty.

The payment made, within the period granted to submit allegations at the opening of the procedure, entails the waiver of any action or administrative appeal against the decision and the recognition of responsibility in relation to the facts referred to in the Agreement to Initiate Penalty Proceedings.

LEGAL GROUNDS

I
Competence and applicable law

In accordance with Articles 58.2 and 60 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR), and pursuant to Articles 47, 48.1, 64.2 and 68.1 and 68.2 of Organic Law 3/2018 of 5 December on the protection of personal data and the guarantee of digital rights (hereinafter LOPDGDD), the Director of the Spanish Data Protection Agency is competent to initiate and decide on this procedure.

Article 63 (2) of the LOPDGDD also states that: '*The procedures handled by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, of this organic law, by the regulatory provisions dictated in their development and, insofar as they are not contradicted, alternatively, by the general rules on administrative procedures*'.

II
Preliminary remarks

In the present case, in accordance with Article 4 (1) and 4 (2) of the GDPR, the processing of personal data is taking place, since WALLBOX collects and stores, inter alia, the following personal data of natural persons: first name, surname and e-mail, among other processing.

WALLBOX carries out that activity in its capacity as controller, since it determines the purposes and means of that activity, pursuant to Article 4 (7) of the GDPR. In addition, this is a cross-border processing, given that WALLBOX has its main establishment in Spain, although it serves other countries of the European Union.

Article 56 (1) of the GDPR provides, for cases of cross-border processing, as provided for in Article 4 (23) thereof, in relation to the competence of the lead supervisory authority, that, without prejudice to Article 55, the supervisory authority of the main establishment or of the sole establishment of the controller or processor shall be competent to act as lead supervisory authority for cross-border processing carried out by that controller or processor in accordance with the procedure laid down in Article 60. In the case under consideration, as explained above, WALLBOX has its main establishment in Spain, so the Spanish Data Protection Agency is competent to act as the lead supervisory authority.

Article 4 (12) GDPR broadly defines *'personal data breach' (hereinafter 'the* security *breach*') as *'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.*

In the present case, there is a personal data security breach in the above circumstances, categorised as a confidentiality breach, as an email was sent without concealing the complainant's email.

Within the principles of processing set out in Article 5 GDPR, the integrity and confidentiality of personal data are guaranteed in Article 5 (1) (f) GDPR. Personal data security is regulated in Articles 32, 33 and 34 of the GDPR, which regulate the security of processing, the notification of a personal data breach to the supervisory authority, and the communication to the data subject, respectively.

III
Principle of integrity and confidentiality

Article 5 (1) (f)*'Principles relating to processing of personal data'* of the GDPR provides:

'1. Personal data shall be:
(...)

> *(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*

In the present case, it is common ground that the complainant's personal data contained in WALLBOX's database were unduly exposed to third parties by sending an email without concealing [redacted] address. In addition, the complainant has been able to access the names and emails of 4 data subjects who replied to the first message in question using the option of Reply all.

As has been established in the file, an email was sent manually to 65 persons, in response to a request for generic information from the data subjects and the complainant's email address was included in field CC and not BCC, so that it was accessible to those 64 other persons. In addition, 4 of these persons replied to the complainant and the complainant was therefore able to access their names and e-mails.

In accordance with the evidence provided for in this final decision, it is considered that the known facts constitute an infringement, attributable to WALLBOX, of Article 5 (1) (f) of the GDPR.

IV
Classification of the infringement of Article 5 (1) (f) GDPR

The aforementioned infringement of Article 5 (1) (f) of the GDPR involve the commission of the infringements referred to in Article 83 (5) of the GDPR, which, under the heading *'General conditions for imposing administrative* fines', provides:

'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

> *(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;; (...)'*

For the purposes of the limitation period, Article 72 *'Very serious infringements'* of the LOPDGDD states:

'1. In accordance with article 83.5 of Regulation (EU) 2016/679, any infringement consisting on a substantial infringement of the provisions mentioned therein, especially the ones listed below, shall be considered very serious infringements and its limitation period shall be three years:

> *(a) The processing of personal data which infringes the principles and guarantees provided for in article 5 of Regulation (EU) 2016/679. (...)'*

V
Sanction for infringement of Article 5 (1) (f) GDPR

For the purposes of deciding on the imposition of an administrative fine and its amount, in accordance with the evidence available at this stage of final decision, it is considered that the penalty to be imposed should be graduated in accordance with the following criteria laid down in Article 83 (2) of the GDPR:

As aggravating factors:

> — The nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them (paragraph a): for displaying the complainant's email address to another 64 persons and for sharing with the complainant the names and emails of some 4 persons.

The assessment of the circumstances referred to in Article 83 (2) of the GDPR, with regard to the infringement of Article 5 (1) (f) of the GDPR, makes it possible to set a penalty of 5,000 EUR (five thousand euros).

VI
Security of processing

Article 32 '*Security of* processing' of the GDPR provides:

'1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and

severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.'

In the present case, at the time of the breach, it has not been established that WALLBOX had appropriate measures to prevent e-mails from being sent without using the CCO functionality, nor had any particular diligence been exercised when sending massive e-mails.

In accordance with the evidence provided for in this final decision, it is considered that the facts known constitute an infringement, attributable to WALLBOX, of Article 32 of the GDPR.

VII

Classification of the infringement of Article 32 GDPR

The aforementioned infringement of Article 32 of the GDPR involve the commission of the offences referred to in Article 83 (4) of the GDPR, which, under the heading *'General conditions for imposing administrative* fines', provides:

'Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (...)'

For the purposes of the limitation period, Article 73 *'Serious infringements'* of the

LOPDGDD states:

'In accordance with article 83.4 of Regulation (EU) 2016/679, any infringement consisting on a substantial infringement of the provisions mentioned therein, especially the ones listed below, shall be considered serious infringements and its limitation period shall be two years:

> *(f) Failure to adopt appropriate technical and organizational measures for ensuring a security level appropriate to the risk related to the processing, in the terms required by article 32.1 of Regulation (EU) 2016/679. (...)'*

VIII
Sanction for infringement of Article 32 GDPR

For the purposes of deciding on the imposition of an administrative fine and its amount, in accordance with the evidence available at the present time of final decision, it is considered that the penalty to be imposed should be graduated in accordance with the following criteria laid down in Article 83 (2) of the GDPR:

As aggravating factors:

— The nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them (paragraph a): for the absence of appropriate measures to prevent the sending of emails containing addresses of recipients without a hidden copy, which may result in the other recipients accessing their contact details and allowing more information on the recipients to be shared when replying with Reply all, which in the present case left the complainant's contact details exposed to 64 other persons and allowed the complainant to access the name, surname and email of another 4 persons.

— The intentional or negligent character of the infringement (paragraph b): WALLBOX's action was seriously negligent in that, having been aware of the situation, the complainant was told that nothing was going to happen, but there is no evidence that, following the complainant's response, the breach in question had been investigated and a solution implemented to prevent such situations from recurring. In fact, the report submitted to this Agency was drawn up precisely following a request for information, but it does not appear that, prior to the Agency's intervention, the company had taken action to analyse what had happened or to adopt preventive or mitigating measures.

Taking into account the circumstances referred to in Article 83 (2) of the GDPR and 76.2 of the LOPDGDD, with regard to the infringement of Article 32 of the GDPR, a penalty of 3,000 EUR (three thousand euros) is set.

IX
Termination of proceedings

Article 85 of Spanish Law 39/2015 of 1 October 2015 on the Common Administrative Procedure of Public Administrations (LPACAP), entitled '*Termination in penalty* proceedings', provides:

'*1. If the offender recognises his or her responsibility, the proceedings may be resolved by imposing the appropriate penalty.*

2. Where the penalty is of a purely financial nature or where a financial penalty and a non-pecuniary penalty may be imposed, but the latter is justified, voluntary payment by the alleged person, at any time prior to the decision, shall entail the termination of the proceedings, except as regards the restoration of the altered situation or the determination of compensation for the damage caused by the infringement. (…)'

According to the above,
The Director of the Spanish Data Protection Agency DECIDES TO**:**

FIRST: DECLARE the termination of proceedings **EXP202204552**, in accordance with Article 85 of the Spanish LPACAP.

SECOND: NOTIFY this decision **WALL BOX CHARGERS S.L.**

In accordance with the provisions of Article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this decision, which terminates the administrative procedure in accordance with the provisions of Article 114.1 (c) of Law 39/2015 of 1 October on the Common Administrative Procedure of Public Administrations, interested parties may lodge an administrative appeal with the Administrative Appeals Chamber of the National High Court, in accordance with Article 25 and paragraph 5 of the fourth additional provision of Law 29/1998 of 13 July governing the administrative courts, within two months from the day following notification of this act, in accordance with Article 46 (1) of that Law.

936-040822

Mar España Martí
Director of the Spanish Data Protection Agency