

- Procedure No.: PS/00038/2019

938-051119

RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and
based on the following

BACKGROUND

FIRST: On October 17, 2018, Ms. AAA, (hereinafter, the claimant
or Ms. EAL), filed a claim with the Spanish Agency for Data Protection
against the entity HOFMANN, S.L.U., (hereinafter, the claimed party), for the following
facts:

-

Deliver to a third party an album with 110 photographs with images of the
claimant, also providing said third party with the telephone number and full name of the
claimant.

-

Provide the claimant in an email reply to one of their
complaints copy of a chat that contained the name and surname of another client of the
reclaimed.

In relation to the facts object of the claim, the claimant points out:

That on August 26, 2018, he hired the respondent to print a
digital album, order to which the reference number ***REFERENCE.1 was assigned, and
which was delivered to his address at ***ADDRESS.1. That being open said
album dated September 20, 2018 found that the print was not correct,
reason why after a complaint he returned to receive a second copy, which also turned out
defective.

As two new complaints made via online were not addressed by the respondent, line, the claimant contacted the respondent by phone on October 3, 2018, being attended by a person who requested a new copy when verifying that it was a printing problem and who, according to the complainant, realized that "for some internal error the shipping address had been changed", showing an address corresponding to another city, an error that said interlocutor "proceeded to change it manually and assured that he would follow the case personally."

That on October 5, 2018, he received an email from the person claimed under the title SENDING, Shipping notification ***ENVIO.1, in which it was indicated that the album would be delivered on October 8, 2018, although it was not until October 10, 2018 that, upon rereading the message because he had not received the order, he verified that in it the ***ADDRESS.2 appeared as the delivery address of the shipment, town in the province of Barcelona in which the order was delivered to a third party alien to his person and in a different address from his own in the city of ***LOCATION.1.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

2/9

That in view of the foregoing, filed new claims before the claimed online and on Facebook. The claimant states that through email the complained indicates: "that they do not know that they have sent any package to my address (something obvious, since they have sent it to ***LOCATION.2).

The person who attends to me, responds to the name of B.B.B., adds between his answers probably by mistake (compromised privacy of this person), a

chat with another person who responds to both A.A.A. as in the name of C.C.C. according to the system, whoever complains about having received an album in which half of the photos are not his; the person with whom the defendant company has crossed the data and to which access to images of my person has been provided, telephone and full name. On 10/10, after 3 emails, I am told to proceed looking for my order to withdraw it. As of 10/16, my order has not been located and my images and personal data are still in the hands of unidentified third parties the use that can be made of these is unknown.”

SECOND: In accordance with article 9.4 of Royal Decree-Law 5/2018, dated On November 2, 2018, said claim was notified to the respondent, who was required the referral within a month from the receipt of the document, among others, of the following information: indication of the causes that motivated the events that originated the claim and specification of the measures adopted to prevent situations similar to the one described above occur. This letter was notified to claimed by electronic means on November 8, 2018, in accordance with appears in the certificate issued by the Notification Service Support service Electronics and Authorized Electronic Address of the National Currency Factory and Stamp-Royal Mint.

Once said period has elapsed, not appearing in the Subdirectorate General for Data Inspection that the respondent had answered the request for information made, dated December 13, 2018, it was proceeded to reiterate the same to the claimed, that after receiving it with that same date by electronic means, as stated in the certificate issued by the aforementioned Notification Service Electronic, did not respond to it within ten business days, counted from the following to its notification, granted for such purposes.

THIRD: Accessed on May 17, 2019, the application of the AEPD that manages

the consultation of antecedents of sanctions and previous warnings in matters

of data protection, it is verified that the claimed party does not have previous records.

FOURTH: On May 27, 2019, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimant,

in accordance with the provisions of article 58.2.b) of Regulation (EU) 2016/679 of the

European Parliament and of the Council of April 27, 2016, regarding the protection of

individuals with regard to the processing of personal data and the free

circulation of these data, (hereinafter RGPD), due to the alleged infringement of article

5.1.f) of the RGPD, typified in article 83.5.a of the same regulation.

Likewise, for the purposes provided in article 58.2.d) of the RGPD in said

The initial agreement notified the corrective measures that, if confirmed

www.aepd.es

C/ Jorge Juan, 6

28001 – Madrid

sedeagpd.gob.es

3/9

existence of infraction, could be imposed in the resolution adopted,

consistent, in view of the elements of judgment available at that time, in

order the implementation of appropriate technical and organizational measures to

guarantee an adequate level of security against the risk of leakage or access

improperly by third parties not interested in the personal data contained in their

systems due to the different treatment operations carried out, this in

order to comply with the principle of data confidentiality. These measures

they would have to be adopted, where appropriate, within the term indicated in the resolution

sanctioning to count from the day following that in which its practice was carried out.

notification, and must provide the means of evidence accrediting its

compliance.

This act was notified to the respondent by electronic means on the 28th of May 2019.

FIFTH: On April 24, 2019, the respondent filed a brief with allegations stating that in view of it, the AEPD, apparently, had not received the documentation submitted in file E/08393/2018 through the headquarters electronically, as evidenced by the acknowledgment of receipt dated December 5, 2018 of your attached presentation.

Located the answering brief referred to by the respondent in his allegations, it is verified that, indeed, he entered this Agency in the date outlined by the respondent, although as it contains documentation referring to a possible breach of personal data security was attached to the unit of the Agency in charge of such matters.

In the aforementioned brief, the respondent answered the request for information that was made together with the transfer of the claim, meaning that "the client (EA) made an order that she received badly cut, it was repeated and she received it again wrong, and it was repeated a third time. This third time it was sent by mistake to someone else (there was a data crossover in that replay in the production database). To the deliver it to the wrong address was rejected and returned to the factory and immediately was forwarded to the correct address, being delivered on 06-11-2018.

Attached to this:

- PDF with the correspondence with the client prior to the claim.
- Security Breach Protocol activated. The fact that it has occurred it is a security incident and, although it does not have the character of a "Security Breach" according to art. 33 GDPR, has also been treated as an internal problem that has been registered, managed and resolved.

- Delivery notes of the 3 shipments that were made to the EA client.

In short, the case was solved and the traceability in the databases so that this error does not occur again. An evaluation of the risk that this incident supposes and it is concluded that it is not necessary to notify the AEPD nor the affected party, as can be seen in Annex 2.”

SIXTH: On November 19, 2019, a resolution proposal was formulated, in the sense that by the Director of the Spanish Agency for Data Protection www.aepd.es

C/ Jorge Juan, 6

28001 – Madrid

sedeagpd.gob.es

4/9

impose a warning sanction on HOFMANN, S.L.U., with NIF B46047502, of in accordance with the provisions of article 58.2.b) of the RGPD, for the alleged infringement of article 5.1.f) of the same rule, typified in article 83.5.a) of the RGPD.

This proposed resolution was notified to the respondent by electronic means dated November 19, 2019.

SEVENTH: On November 29, 2019, entry is registered in this Agency written allegations of the claimed, in which, in addition to exposing his compliance with the sanction of warning indicated in the resolution proposal received, expresses "its firm commitment to the review, reinforcement and updating of the current technical, legal and organizational security measures for the protection of personal data, in particular of the processes directly involved with the order management, identification of recipients, review of final quality before of the delivery process, continuous training of personnel, as well as relations with their treatment managers for the logistics service.”

PROVEN FACTS

First: On October 17, 2018, Ms. EAL filed a claim with the Spanish Data Protection Agency against the entity HOFMANN, S.L.U., (the claimed), for having delivered to a third party at an address and location other than own a digital album with 110 photographs with images of the claimant and also provide said third party with the telephone number and full name of the claimant.

Second: The claimant, residing in the town of ***LOCALIDAD.1, according to appears on his ID, he stated in his claim that on October 5, 2018 received an email from the claimant under the title SENDING, Shipping Notification ***SHIPPING.1, informing him that the album would be delivered to him on the 8th of October 2018 at ***ADDRESS.2.

Third: Enter the documentation provided by the claimed party as maintained with the claimant works transcript of an email sent by the claimant to the claimed on on 10/10/2018, at 05:38 PM, in which it stated to the defendant:

"I have received the email from sending saying that my album, left its facilities has been delivered to the address you have provided in ***LOCATION.2. Their colleague told me on the phone that she was proceeding to request a third album that It would arrive by last Friday. Sending has delivered to someone else this Monday, do you need more evidence? Thanks. A.A.A."

Fourth: In the documentation provided by the respondent regarding the "Protocol of Management and notification of security violations of personal data" is describes that the personal data affected by the shipment of the claimant's order to an incorrect address are the name, telephone and printed images of it.

Likewise, said document states that the respondent adopted in relation to the security violation analyzed the following corrective measures:

a) In the production databases: review of the possible existence of

a data crossing, correction of the affected records and verification of

the integrity of the DB;

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/9

b) In the internal production/intranet database: correction in the

old orders to prevent the claimant's address from being

incorrectly completed.

c) The affected party was informed of the security incident or failure arising from the

sending the album to another address that was not yours and contacted the

person to whom the order had been delivered in order to retrieve it from the object

to deliver it to the correct address, where it was delivered on 11/06/2018.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 55.1, 56.2 and 58.2 of the Regulation (EU)

2016/679 of the European Parliament and of the Council of April 27, 2016, regarding the

protection of natural persons with regard to data processing

personal information and the free circulation of these data (General Protection Regulation

of Data, hereinafter RGPD) recognizes each control authority, and according to what

established in articles 47 and 48.1 of Organic Law 3/2018, of December 5, of

Protection of Personal Data and guarantee of digital rights (hereinafter

LOPDGDD), the Director of the Spanish Data Protection Agency is

competent to resolve this procedure.

II

Article 4 of the RGPD, under the heading "Definitions", provides that: "For the purposes of this Regulation shall be understood as:

1) "personal data": any information about an identified natural person or identifiable ("the interested party"); An identifiable natural person shall be deemed to be any person whose identity can be determined, directly or indirectly, in particular by an identifier, such as a name, an identification number, location, an online identifier or one or more elements of the identity physical, physiological, genetic, psychic, economic, cultural or social of said person;

2) "processing": any operation or set of operations carried out about personal data or sets of personal data, either by procedures automated or not, such as the collection, registration, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, broadcast or any other form of enabling of access, collation or interconnection, limitation, suppression or destruction;"

7) «responsible for the treatment>> or <<responsible>>: the natural person or legal entity, public authority, service or other body which, alone or jointly with others, determine the purposes and means of the treatment; if the law of the Union or of the Member States determines the purposes and means of processing, the data controller treatment or the specific criteria for their appointment may be established by the Law of the Union or of the Member States; >>

“9) <<recipient>>: the natural or legal person, public authority, service or another body to which personal data is communicated, whether or not it is a third party.

However, public authorities that may receive personal data in the context of a specific investigation in accordance with www.aepd.es

with the Law of the Union or of the Member States; the processing of such data

by such public authorities shall be in accordance with the rules on

data protection applicable to the purposes of the treatment;

10) <<third party>>: natural or legal person, public authority, service or

body other than the interested party, the data controller, the person in charge of

treatment and of the persons authorized to treat personal data under the

direct authority of the person in charge or the person in charge; “

In accordance with these definitions, the treatment by the

claimed of the identification data (name and surnames), postal address, telephone

and images (photographs) of the claimant for the purpose of managing the delivery of a

request, constitutes a treatment of personal data, in respect of which the

responsible for the treatment, in this case the claimed, must comply with

the principles relating to treatment, among which is the principle of

confidentiality contained in article 5.1.f) of the RGPD.

III

In the present case, the defendant is charged with a breach of article 5.1. of

RGPD, precept that under the heading "Principles related to treatment", establishes in

its section f) that:

“Personal data will be:

(...)

f) treated in such a way as to ensure adequate security of the

personal data, including protection against unauthorized or unlawful processing and

against its loss, destruction or accidental damage, through the application of measures

appropriate technical or organizational (<<integrity and confidentiality>>)"

For its part, regarding the "Principles of Data Protection", article 5 of

the LOPDGDD, under the heading "Duty of confidentiality", provides:

"1. Those responsible and in charge of data processing as well as all

people who intervene in any phase of this will be subject to the duty of

confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary

of the duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will remain

even when the relationship of the obligor with the person in charge or person in charge had ended

of the treatment."

In the present case, from the assessment of the set of evidence elements

available in the procedure, in particular, of the information contained in the

documentation associated with the "Protocol for the management and notification of violations of

security of personal data" provided by the respondent, it is evident that

In early October 2018, the respondent handed over to a third party in a

address and location other than the city in which the claimant resided a

order that included personal data of the same, so that said

third party accessed the name, surnames, telephone number and images of the claimant who

were included in the order that was delivered to him.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/9

Even in the aforementioned documentation, the fact studied is

described as sending an order to an incorrect address that has affected the name, telephone number and printed images of the claimant, a circumstance that also is reflected from the content of emails maintained between claimed and claimant prior to the filing of a claim with this Agency, appearing in the email sent by the claimant to the claimant on 10/10/2018, at 05:29 PM, the following affirmation of the affected "My photos have been delivered to another person, with my name and phone number.

Therefore, said conduct constitutes, on the part of the defendant, responsible of the aforementioned processing of personal data, a violation of the principle of confidentiality contained in article 5.1.f) of the RGPD, infringement typified in the article 83.5.a) of the aforementioned Regulation and classified as a very serious infraction to effects of prescription in article 72.1.a) of the LOPDGDD, since when delivering the order at an incorrect address was provided to an uninterested third party identification data, telephone number and photographs concerning the claimant.

IV

Sections b), d) and i) of article 58.2 of the RGPD provide the following:

"2 Each supervisory authority shall have all of the following powers corrections listed below:

(...)

b) sanction any person responsible or in charge of the treatment with warning when the processing operations have violated the provisions of this Regulation;"

(...)

"d) order the person responsible or in charge of the treatment that the operations of treatment comply with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;"

“i) impose an administrative fine in accordance with article 83, in addition to or in
instead of the measures mentioned in this paragraph, depending on the circumstances
of each particular case;

Article 83 of the RGPD, under the heading “General conditions for the
imposition of administrative fines”, in sections 1 and 5.a) states that:

“1. Each control authority will guarantee that the imposition of fines
administrative actions under this article for violations of this
Regulation indicated in sections 4, 5 and 6 are in each individual case
effective, proportionate and dissuasive.”

“5. Violations of the following provisions will be sanctioned,
according to paragraph 2, with administrative fines of EUR 20,000,000 as
maximum or, in the case of a company, an amount equivalent to 4% as
maximum of the overall annual total turnover of the previous financial year,
opting for the highest amount:

“a) the basic principles for the treatment, including the conditions for the
consent under articles 5, 6, 7 and 9”

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

8/9

At the same time, article 72.1.a) of the LOPDGDD typifies the infringement of
principle of confidentiality as very serious for prescription purposes in
following terms: “1. Based on the provisions of article 83.5 of the Regulation
(EU) 2016/679 are considered very serious and will prescribe after three years the
infractions that suppose a substantial violation of the mentioned articles

in that and, in particular, the following:

a) The processing of personal data violating the principles and guarantees established in article 5 of Regulation (EU) 2016/679.”

In the present case, and without prejudice to the measures adopted by the claimed to correct the irregular situation as responsible for the treatment, it is considered appropriate to impose the sanction of warning provided for in the article 58.2.b) of the RGPD in view of the following circumstances: that the treatment irregular analyzed would only affect the personal data of two clients of the claimed (the claimant and the third party who had access to the information) that have been seen immersed in the situation described, at the same time that it is considered that the fine administrative that could fall in accordance with the provisions of article 83.5.a) of the RGPD would constitute a disproportionate burden for the claimed party, who is not aware the commission of any previous infringement in terms of data protection.

Confirmed the infraction described, the defendant has justified before this Agency through the documentation provided that, together with the steps taken to recover the order delivered to the wrong address and send the album to your right direction, have adopted a series of technical and organizational measures in order to correct the detected security flaw, which affected the records referred to two clients, also proceeding to review the database of production to check its integrity. It has also communicated its commitment in reviewing, reinforcing and updating such measures in order to comply with the principle of confidentiality of the treatment and protect the rights of the interested parties.

Therefore, in accordance with the applicable legislation and valued the concurrence of the facts whose existence has been proven,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE HOFMANN, S.L.U., with NIF B46047502, in accordance with

the provisions of article 58.2.b) of the RGPD, a sanction of warning for a
infringement of article 5.1.f) of the RGPD, typified in article 83.5.a) of the RGPD.

SECOND: NOTIFY this resolution to HOFMANN, S.L.U., with NIF
B46047502.

In accordance with the provisions of article 50 of the LOPDGDD, the

This Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art.

48.6 of the LOPDGDD, and in accordance with the provisions of article 123 of the

LPACAP, the interested parties may optionally file an appeal for reconsideration

before the Director of the Spanish Agency for Data Protection within a period of

month from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-Administrative Chamber of the

www.aepd.es

C/ Jorge Juan, 6

28001 – Madrid

sedeagpd.gob.es

9/9

National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the

Contentious-administrative jurisdiction, within a period of two months from the

day following the notification of this act, as provided in article 46.1 of the

aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the

LPACAP, the firm resolution may be provisionally suspended in administrative proceedings

if the interested party expresses his intention to file a contentious appeal-

administrative. If this is the case, the interested party must formally communicate this

made by writing to the Spanish Agency for Data Protection,

introducing him to

the agency

[<https://sedeagpd.gob.es/sede-electronica-web/>], or through any of the other

records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. Also

must transfer to the Agency the documentation that proves the effective filing

of the contentious-administrative appeal. If the Agency were not aware of the

filing of the contentious-administrative appeal within two months from the

day following the notification of this resolution, it would end the

precautionary suspension.

Electronic Registration of

through the

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es