

□ Procedure No.: EXP202100066 (PS/00404/2022)

RESOLUTION OF THE SANCTION PROCEDURE

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

BACKGROUND

FIRST: On 06/04/21, a document submitted by

Mrs. A.A.A., (hereinafter, "the claiming party"), against the entity, CASA 7

PERSONAL SHOPPER, S.L., with CIF.: B87396172, (hereinafter "the part

claimed"), in which it indicated, among other things, the following:

"I have requested information for an advertisement published by this company about
a sale that they manage and the response has included the mail of
several people and we have all received it. They have not used the blind copy
so all emails are visible to all of us who have received the
same answer, in total (...) people. It does not seem logical to me that my address
mail has no one I don't know and even less who knows what they are
my personal interests because my email address also includes my
real name".

The claim document is accompanied by the following relevant documentation for the
present procedure:

- Copy of the email sent on 06/02/21, from the address

***USER.1@gmail.com to (...) recipients without hiding their email addresses

mail (without using the BCC functionality), with information related to a
plot of the Urbanization (...).

SECOND: On 07/21/21 and 08/09/21, in accordance with the provisions of the

Article 65.4 of Organic Law 3/2018, of December 5, on Data Protection

Personal Rights and Guarantee of Digital Rights (LOPDGDD), by this

Agency, said claim was transferred to the claimed party, so that

proceed to its analysis and report, within a month, on what was exposed

in the claim letter.

- According to the certificate of the Electronic Notifications and Electronic Address Service

e-mail, the application document sent to the claimed party, on 07/21/21, to

through the electronic notification service "NOTIFIC@", was rejected

at destination on 08/01/21.

- According to the certificate of the State Postal and Telegraph Society, the letter of support

legality sent to the claimed party, on 08/09/21 through the service of no-

Postal notifications from Correos, was returned to its destination with the annotation of

"a stranger".

THIRD: On 09/21/21, by the Director of the Spanish Agency for

Protection of Data, an agreement is issued to admit the processing of the claim

presented, in accordance with article 65 of the LPDGDD Law, when assessing possible

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

2/7

rational indications of a violation of the rules in the field of competences

of the Spanish Data Protection Agency

FOURTH: On 05/09/22, 05/30/22 and 06/28/22, the General Subdirectorate of

Data Inspection proceeded to make a request for information to the party

claimed, by virtue of the investigative powers granted to the authorities of

control in article 58.1 of Regulation (EU) 2016/679, of the European Parliament and

of the Council, of 04/27/16, regarding the Protection of Physical Persons in what
regarding the Processing of Personal Data and the Free Circulation of these Data
(GDPR) and in accordance with the provisions of Title VII, Chapter I, Section
second, of the LOPDGDD.

- According to the certificate of the Electronic Notifications and Electronic Address Service
e-mail, the application document sent to the claimed party, on 05/09/22, to
through the electronic notification service "NOTIFIC@", was rejected
at destination on 05/20/22.

- According to the certificate of the State Postal and Telegraph Society, the letter of support
legality sent to the claimed party, on 05/30/22 through the service of no-
postal notifications from Correos, was returned to its destination with the annotation "au-
sente of the cast", and not having received the notification from the "List" service of
Mail.

- According to the certificate of the State Postal and Telegraph Society, the letter of support
legality sent to the claimed party, on 06/28/22 through the service of no-
Postal notifications from Correos, was received at destination on 07/14/22.

The letter granted the claimed party a period of ten business days to
answer the request. This period ended on 07/29/22 and as of today, no
received in this Agency any type of response to the request for information
required.

FIFTH: On 08/08/22, the Director of the Spanish Agency for the Protection of
Datos agreed to initiate disciplinary proceedings against the claimed party, for the alleged
violation of Article 5.1.f) of the GDPR, imposing an initial penalty of 2,000 euros
(two thousand euros), and for violation of article 32 of the GDPR, imposing a sanction
initial amount of 1,500 euros (one thousand five hundred euros).

- According to the certificate of the State Postal and Telegraph Society, the letter of

initiation of file sent to the claimed party, on 08/11/22 through
of the postal notification service of Correos, was returned to its destination on
08/29/22 with the annotation "absent from the distribution", and not having collected the
notification of the Mail "List" service.

In accordance with article 44 of Law 39/2015, of October 1, of the PACAP Law, when
having been unsuccessful the practice of notification of the indicated act, it is
publishes announcement in the Official State Gazette dated 08/31/22.

SIXTH: Notified the aforementioned start agreement in accordance with the rules established in
the LPACAP and after the period granted for the formulation of allegations, it has been

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/7

It has been verified that no allegation has been received by the claimed party to said
agreement.

Article 64.2.f) of the LPACAP -provision of which the claimed party was informed
in the agreement to open the procedure - establishes that if no
arguments within the established term on the content of the initiation agreement, when
it contains a precise pronouncement about the imputed responsibility,
may be considered a resolution proposal. In the present case, the agreement of
beginning of the disciplinary file determined the facts in which the
imputation, the infringement of the GDPR attributed to the defendant and the sanction that could
impose. Therefore, taking into consideration that the claimed party has not
made allegations to the agreement to start the file and in attention to what
established in article 64.2.f) of the LPACAP, the aforementioned initiation agreement is

considered in the present case resolution proposal.

In view of all the proceedings, by the Spanish Agency for Data Protection

In this proceeding, the following are considered proven facts:

PROVEN FACTS

Of the actions carried out in this procedure, it has been accredited

the following facts:

First: As has been verified, the claimant received an email

sent on 06/02/21, from the address ***USUARIO.1@gmail.com in which

I could read the addresses of other (...) recipients, who were not hiding. This is the \ It \ him

sending had been made without using the BCC functionality of the email, which

made it possible for all recipients to have access to the email address of the

the rest.

FUNDAMENTALS OF LAW

I.- Competition:

It is competent to initiate and resolve this procedure, the Director of the Agency

Spanish Data Protection Agency, by virtue of the powers that article 58.2 of the GDPR

recognizes each Control Authority and, as established in arts. 47, 64.2 and

68.1 of the LOPDGDD Law.

II.- Summary of the facts:

In the documentation provided by the claimant, it can be seen that, on 06/02/21 to

5:28 p.m., from the email address, ***USER.1@gmail.com,

whose owner is the entity CASA 7 PERSONAL SHOPPER, S.L., an email was sent

mail to (...) recipients whose addresses appeared in it without being

hidden, that is, the BCC functionality had not been used in it.

III.- On the lack of confidentiality in the processing of personal data.

C / Jorge Juan, 6

Article 5 of the GDPR establishes the principles that must govern the treatment of personal data.

personal data and mentions, in section 1.f) that of "integrity and confidentiality":

"1. Personal data will be: f) treated in such a way as to guarantee a
adequate security of personal data, including protection against
unauthorized or illegal treatment and against its loss, destruction or damage
accidental, through the application of technical or organizational measures
("integrity and confidentiality").

In the case at hand, the defendant, by sending an email without using the
blind copy option has violated confidentiality in data processing
of a personal nature included in article 5.1.f) GDPR, since in this way, the
claimant had access to the email addresses of the rest of the
recipients.

This infraction is sanctioned with a fine of €20,000,000 maximum or, in the case of
of a company, in an amount equivalent to a maximum of 4% of the volume of
overall annual total business of the previous financial year, opting for the one with the highest
amount, in accordance with article 83.5.a) of the GDPR.

For its part, article 72.1.a) of the LOPDGDD considers it very serious, for the purposes of
prescription, "The processing of personal data violating the principles and guarantees
established in article 5 of Regulation (EU) 2016/679".

The balance of the circumstances contemplated in article 83 of the GDPR, with
regarding the offense committed by violating the provisions of its article 5.1.f),
allows a penalty of 2,000 euros (two thousand euros) to be set.

IV.- On the lack of security in the processing of personal data.

Security in the processing of personal data is regulated in article 32

of the GDPR, which establishes that:

"1. Taking into account the state of the art, the application costs, and the nature, scope, context and purposes of processing, as well as risks of variable probability and severity for the rights and freedoms of natural persons, the person in charge and the person in charge of the treatment will apply appropriate technical and organizational measures to ensure a level of security appropriate to the risk, which, if applicable, includes, among others: a) the pseudonymization and encryption of personal data; b) the ability to guarantee the ongoing confidentiality, integrity, availability and resilience of the treatment systems and services; c) the ability to restore the availability and access to personal data quickly in case of physical or technical incident; d) a process of verification, evaluation and assessment regular monitoring of the effectiveness of technical and organizational measures to ensure the safety of the treatment.

2. When evaluating the adequacy of the level of security, particular attention should be paid to take into account the risks presented by data processing, in particular as consequence of the destruction, loss or accidental or unlawful alteration of

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/7

personal data transmitted, stored or processed in another way, or the unauthorized communication or access to such data.

3. Adherence to an approved code of conduct pursuant to article 40 or to a certification mechanism approved under article 42 may serve as element to demonstrate compliance with the requirements established in the paragraph 1 of this article.

4. The person in charge and the person in charge of the treatment will take measures to ensure that any person acting under the authority of the controller or of the person in charge and has access to personal data can only process such data following the instructions of the person in charge, unless it is obliged to do so under the law of the Union or of the Member States”.

It should be noted that the GDPR in the aforementioned precept does not establish a list of the security measures that are applicable according to the data that is the object of treatment, but it establishes that the person in charge and the person in charge of the treatment apply technical and organizational measures that are appropriate to the risk involved the treatment, taking into account the state of the art, the application costs, the nature, scope, context and purposes of processing, probability risks and seriousness for the rights and freedoms of the persons concerned.

In addition, security measures must be adequate and proportionate to the detected risk, noting that the determination of the technical measures and organizational procedures must be carried out taking into account: pseudonymization and encryption, the ability to ensure confidentiality, integrity, availability and resilience, the ability to restore availability and access to data after an incident, process verification (not audit), evaluation and assessment of the effectiveness of the measures.

In any case, when evaluating the adequacy of the security level, particular account of the risks presented by data processing, such as consequence of the destruction, loss or accidental or illegal alteration of data

personal information transmitted, preserved or processed in another way, or the communication or unauthorized access to said data and that could cause damages physical, material or immaterial.

In the case at hand, the defendant, by sending an email without using the blind carbon copy option is in breach of its obligation to apply the technical measures and organizational procedures to guarantee an adequate level of security in the treatment of personal data included in article 32 GDPR.

This infraction can be sanctioned with a fine of a maximum of €10,000,000 or, in the case of a company, an amount equivalent to a maximum of 2% of the total annual global business volume of the previous financial year, opting for the of greater value, in accordance with article 83.4.a) of the GDPR.

For its part, Article 73.f) of the LOPDGDD considers serious, for the purposes of prescription, "f) The lack of adoption of those technical and organizational measures that are appropriate to guarantee a level of security appropriate to the risk of the

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

6/7

treatment, in the terms required by article 32.1 of the Regulation (EU) 2016/679.”.

The balance of the circumstances contemplated in article 83 of the GDPR, with regarding the infringement committed by violating the provisions of article 32 of the GDPR, allows a penalty of 1,500 euros (one thousand five hundred euros) to be set.

Therefore, in accordance with the foregoing, and with the applicable legislation, the Director of the Spanish Data Protection Agency,

RESOLVES:

FIRST: IMPOSE the entity CASA 7 PERSONAL SHOPPER, S.L., with CIF.:

B87396172 for violation of article 5.1.f) of the GDPR, when sending an email

email violating the confidentiality of the recipients, with a sanction of

2,000 euros (two thousand euros) and for the violation of article 32 of the GDPR, when sending a

email without using the blind copy option, that is, without applying the measures

appropriate technical and organizational measures to guarantee an adequate level of security,

with a penalty of 1,500 euros (one thousand five hundred euros)

SECOND: NOTIFY this resolution to CASA 7 PERSONAL SHOPPER,

S.L.

THIRD: Warn the penalized party that the sanction imposed must make it effective

once this resolution is enforceable, in accordance with the provisions of Article

Article 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (LPACAP), within the voluntary payment term

indicated in article 68 of the General Collection Regulations, approved by Royal

Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003, of 17

December, by depositing it in the restricted account No. ES00 0000 0000 0000

0000 0000, opened in the name of the Spanish Data Protection Agency in the

Banco CAIXABANK, S.A. or otherwise, it will proceed to its collection in

executive period.

Once the notification has been received and once executed, if the execution date is

between the 1st and 15th of each month, both inclusive, the term to make the payment

voluntary will be until the 20th day of the following or immediately following business month, and if

between the 16th and the last day of each month, both inclusive, the payment term

It will be until the 5th of the second following or immediately following business month.

In accordance with the provisions of article 82 of Law 62/2003, of 30

December, of fiscal, administrative and social order measures, the present Resolution will be made public, once the interested parties have been notified. The publication will be made in accordance with the provisions of Instruction 1/2004, of 22 December, from the Spanish Agency for Data Protection on the publication of their Resolutions.

Against this resolution, which puts an end to the administrative process, and in accordance with the established in articles 112 and 123 of the LPACAP, interested parties may file, optionally, an appeal for reversal before the Director of the Agency

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/7

Spanish Data Protection Agency within a period of one month from the day following the notification of this resolution, or, directly, a contentious appeal before the Contentious-Administrative Chamber of the National Court, in accordance with the provisions of article 25 and paragraph 5 of the provision additional fourth of Law 29/1998, of 07/13, regulating the Jurisdiction Contentious-administrative, within a period of two months from the day following to the notification of this act, as provided in article 46.1 of the aforementioned text legal.

Finally, it is noted that in accordance with the provisions of art. 90.3 a) of the LPACAP, may provisionally suspend the firm resolution in administrative proceedings if the The interested party expresses his intention to file a contentious-administrative appeal. If this is the case, the interested party must formally communicate this fact through writing addressed to the Spanish Data Protection Agency, presenting it through

of the Electronic Registry of the Agency [<https://sedeagpd.gob.es/sede-electronicaweb/>],
or through any of the other records provided for in art. 16.4 of the aforementioned Law
39/2015, of October 1. You must also transfer the documentation to the Agency
proving the effective filing of the contentious-administrative appeal. if the
Agency was not aware of the filing of the contentious appeal-
administration within a period of two months from the day following the notification of the
present resolution, would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es