 Procedure No.: PS/00007/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following:

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claimant) dated August 31, 2018

filed a claim with the Spanish Data Protection Agency. The

The claim is directed against Management and Administration of Receipts S.A. with CIF

A83052621 (hereinafter, the claimed).

The reasons on which the claim is based are that on August 30, 2018 it is received in

multiple email mailboxes, even in another company's mailboxes, one email

from “***EMAIL.1” addressed to the claimant so that he can contact

BBVA in relation to a financing that it maintains with that entity.

The complainant adds that the contact address he provided to BBVA is not the

corporate management of MAPFRE but the personal one of GMAIL.

Provide the following documentation:

- Email from “***EMAIL.1” addressed to the email address

“***EMAIL.2” and copying the addresses “***EMAIL.3” and “***EMAIL.4”.

SECOND: In view of the facts denounced in the claim and the

documents provided by the claimant and the facts and documents of which he has

had knowledge of this Agency, the Subdirectorate General for Data Inspection

proceeded to carry out preliminary investigation actions for the

clarification of the facts in question, by virtue of the investigative powers

granted to the control authorities in article 57.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter RGPD), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the Law Organic 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter LOPDGDD).

As a result of the research actions carried out, it is found that the responsible for the treatment is the claimed.

In addition, the following extremes are noted:

On November 21, 2019, in procedure E/06909/2018, the Agency Spanish Data Protection agreed to carry out the actions of investigation carried out in file E/00730/2019 in relation to the facts claimed.

During these proceedings it was verified that the claimant had provided the corporate address from Mapfre to BBVA. Likewise, it was concluded that the defendant forwarded the claimed email to mailboxes other than the claimant.

After twelve months without being able to conclude the proceedings necessary to clarify the possible responsibilities of the claimed facts, dated December 3, 2019, in procedure E/00730/2019, the Agency Spanish Data Protection Agency agreed to file the proceedings and open these investigative actions, attached to file E/11745/2019.

Requested from BBVA the specific service contract maintained with OPPLUS, with date of July 8, 2020 is received in this Agency, with registration number 023874/2020, the required service provision contract submitted by this entity.

Information requested from the MAPFRE entity on the causes that led to the error
of delivery to the claimant of the mail sent from "...***EMAIL.1" and information and
purpose of mailboxes “***EMAIL.5” and “***EMAIL.4”, the latter belonging to another
company, where it is requested that a copy of the message be sent in case of error, with
date of July 8, 2020 is received in this Agency, with registration number
023956/2020, brief of allegations stating that the claimant does not keep
any relationship with this entity and urging this Agency to address the request for
information to the entity MAPFRE TECH, as this is, possibly, the entity
responsible for processing the data of the claimant in the facts referred to
your claim.

The same information indicated in the previous paragraph was requested from the MAPFRE entity
TECH, dated October 22, 2020, is received in this Agency, with the number of
registration ***REGISTRATION.1, brief of allegations sent by this entity
stating the following aspects:

- Regarding the delivery error of the mail sent by “garsa.opplus.bbva.com” that
triggered the facts claimed, this was due to the transfer, dated
April 1, 2018, by MAPFRE TECH to IBM GLOBAL SERVICES ESPANA, S.A. (in
hereinafter, IBM GSE) of the productive unit in which the claimant lent his
services, for which the claimant ceased to be an employee of MAPFRE TECH passing
to be an employee of IBM GSE, maintaining their labor rights and obligations in
the legally regulated terms. Being already an external employee of MAPFRE, he was
I assign a new email account (...***EMAIL.6) with the domain
designated for external personnel of other companies that provide services to
MAPFRE, programming the delivery error message in your old mailbox
received by GYAR. They add at this point that the email provided by MAPFRE to its
employees is for exclusively professional use as expressly indicated

in the informative clause of access to its computer systems that all users

You must accept in order to continue with the system boot process:

“You are accessing an Information Processing System

owned by MAPFRE. Access to and use of this system is permitted.

exclusively to authorized persons and for strictly

professionals."

As in the confidentiality clause that establishes the obligation of employees

regarding this matter that was accepted by the claimant:

"Computing resources, such as email and the Internet, are a

work tool provided by the MAPFRE Group to its employees, therefore

that its use will be limited to the functions associated with the development of the activity

user's professional, the employee being aware of the prohibition of

use them for private purposes or unrelated to the performance of their activity

employment, the company being able to carry out as many acts of investigation, registration

[…]”

- Regarding the function of the mailbox "***EMAIL.5" they state that it is a mailbox

internal MAPFRE TECH created for the correct transition from MAPFRE TECH to

IBM GSE of the services covered by the outsourcing contract to ensure that they do not

there were unanswered service requests. They add that they do not know why

that BBVA sent a message to this mailbox despite the fact that in the mail returned with an error

The delivery box expressly identifies that it is a service mailbox.

Finally, they indicate that six MAPFRE employees have access to this mailbox

TECH in charge of the supervision and control of the adequate transition of the

outsourcing services from MAPFRE to IBM GSE.

- Regarding the function of the mailbox "***EMAIL.4" it is an operational mailbox of IBM

GSE with the same function and purpose as in the previous case but managed by the

receiving company of the outsourcing that is also expressly identified in

the delivery error return mail, which is a service mailbox. add

that this mailbox has access to ten IBM GSE employees responsible for the

supervision and control of the proper transition of outsourcing services.

The statement made by the claimant that the email address

provided to BBVA is only the one corresponding to "gmail.com" is not correct as

it was demonstrated within file E/00730/2019.

The use of computer media provided by Mapfre was accepted

by the claimant as for professional use only, thus excluding the

function of Mapfre's email address as a means of contact for other purposes.

The statement made by the claimant that the mail indicated in the

claim had been spread to about three thousand people, it is not correct. It has been

verified in the present investigative actions that this email had

six people from Mapfre Tech with operational functions and ten people from

IBM GSE with same functions.

The entity GYAR, sub-processor contracted by OPPLUS, carried out

sending e-mail about the claimant's financial situation to mailboxes

that clearly did not correspond to the claimant.

From the email that has motivated the claim, and that provides the

claimant, it is verified that one of the IBM GSE employees with access to the

service mailbox “***EMAIL.4”, did not forward the personal email to

claimant, but to a third person from MAPFRE TECH.

THIRD: On January 25, 2021, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimed, for the

alleged infringements of articles 5.1 f) and 32 of the RGPD, typified in articles

83.5 a) and 83.4 a) of the GDPR respectively.

FOURTH: Once the initiation agreement has been notified, the one claimed at the time of this

The resolution has not presented a written statement of allegations, for which reason the

indicated in article 64 of Law 39/2015, of October 1, on the Procedure

Common Administrative Law of Public Administrations, which in section f)

establishes that in the event of not making allegations within the period established on the

content of the initiation agreement, it may be considered a proposal for

resolution when it contains a precise statement about the responsibility

imputed, reason why a Resolution is issued.

FIFTH: Of the actions carried out in this proceeding, they have been

accredited the following:

PROVEN FACTS

FIRST: It is stated that on August 30, 2018 it is received in several mailboxes

email, even in another company's mailboxes, mail from

“***EMAIL.1” addressed to the claimant to contact BBVA at

relation to a financing that it maintains with that entity.

The contact address provided by the claimant to BBVA is not the address

corporate of MAPFRE but the personal one of GMAIL.

- Email from “***EMAIL.1” addressed to the email address

“***EMAIL.2” and copying the addresses “***EMAIL.3” and “***EMAIL.4”.

SECOND: The claimed, sub-processor contracted by OPPLUS,

sent the email about the claimant's financial situation to

mailboxes that clearly did not correspond to the claimant.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each

control authority, and as established in arts. 47 and 48.1 of the LOPDGDD, the

Director of the Spanish Data Protection Agency is competent to resolve

this procedure.

II

Law 39/2015, of October 1, on the Common Administrative Procedure of

the Public Administrations, in its article 64 "Agreement of initiation in the

procedures of a sanctioning nature”, provides:

"1. The initiation agreement will be communicated to the instructor of the procedure, with

transfer of how many actions exist in this regard, and the interested parties will be notified,

understanding in any case by such the accused.

Likewise, the initiation will be communicated to the complainant when the regulatory norms

of the procedure so provide.

2. The initiation agreement must contain at least:

a) Identification of the person or persons allegedly responsible.

b) The facts that motivate the initiation of the procedure, its possible

rating and sanctions that may apply, without prejudice to what

result of the instruction.

c) Identification of the instructor and, where appropriate, secretary of the procedure, with

express indication of the system of recusal of the same.

d) Competent body for the resolution of the procedure and regulation that

attribute such competence, indicating the possibility that the presumed

responsible can voluntarily acknowledge their responsibility, with the

effects provided for in article 85.

e) Provisional measures that have been agreed by the body

competent to initiate the sanctioning procedure, without prejudice to those that

may be adopted during the same in accordance with article 56.

f) Indication of the right to formulate allegations and to the hearing in the

procedure and the deadlines for its exercise, as well as an indication that, in

If you do not make allegations within the stipulated period on the content of the

initiation agreement, this may be considered a resolution proposal

when it contains a precise statement about the responsibility

imputed.

3. Exceptionally, when at the time of issuing the initiation agreement

there are not sufficient elements for the initial qualification of the facts that motivate

the initiation of the procedure, the aforementioned qualification may be carried out in a phase

later by drawing up a List of Charges, which must be notified to

the interested".

In application of the previous precept and taking into account that no

formulated allegations to the initial agreement, it is appropriate to resolve the initiated procedure.

III

The defendant is charged with the violation of articles 5.1 f) and 32 of the RGPD.

The RGPD establishes in article 5 the principles that must govern the treatment

of personal data and mentions among them that of “integrity and confidentiality”.

The article notes that:

"1. The 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").

In turn, the security of personal data is regulated in article 32

of the GDPR.

Article 32 of the RGPD "Security of treatment", establishes that:

"1. Taking into account the state of the art, the application costs, and the

nature, scope, context and purposes of the treatment, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical measures and

appropriate organizational measures to guarantee a level of security appropriate to the risk,

which in your case includes, among others:

a) pseudonymization and encryption of personal data;

b) the ability to ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and evaluation of the effectiveness

technical and organizational measures to guarantee the security of the

treatment.

2. When evaluating the adequacy of the security level, particular consideration shall be given to

taking into account the risks presented by the processing of data, in particular as

consequence of the accidental or unlawful destruction, loss or alteration of data

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data.

3. Adherence to an approved code of conduct under article 40 or to a

certification mechanism approved under article 42 may serve as an element

to demonstrate compliance with the requirements established in section 1 of the

present article.

4. The person in charge and the person in charge of the treatment will take measures to

guarantee that any person acting under the authority of the controller or the

manager and has access to personal data can only process said data

following the instructions of the person in charge, unless it is obliged to do so by virtue of the

Law of the Union or of the Member States".

The violation of article 32 of the RGPD is typified in article 83.4.a)

of the aforementioned RGPD in the following terms:

"4. Violations of the following provisions will be sanctioned, in accordance

with paragraph 2, with administrative fines of a maximum of EUR 10,000,000 or,

in the case of a company, an amount equivalent to a maximum of 2% of the

global total annual turnover of the previous financial year, opting for

the largest amount:

a) the obligations of the person in charge and the person in charge pursuant to articles 8,

11, 25 to 39, 42 and 43.

(…)"

For its part, the LOPDGDD in its article 71, Violations, states that:

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result

contrary to this organic law.

And in its article 73, for the purposes of prescription, it qualifies as "Infringements

considered serious":

"Based on the provisions of article 83.4 of Regulation (EU) 2016/679

are considered serious and will prescribe after two years the infractions that suppose a

substantial violation of the articles mentioned therein and, in particular, the

following:

(…)

g) The violation, as a consequence of the lack of due diligence,

of the technical and organizational measures that have been implemented in accordance with

required by article 32.1 of Regulation (EU) 2016/679".

III

The GDPR defines personal data security breaches as

“all those violations of security that cause the destruction, loss or

accidental or unlawful alteration of personal data transmitted, stored or processed

otherwise, or unauthorized communication or access to such data”.

From the documentation in the file, there are clear indications of

that the claimed party has violated article 32 of the RGPD, when there was a breach of

security in their systems since it is received in several mailboxes

email, even in another company's mailboxes, mail from

“***EMAIL.1” addressed to the claimant to contact BBVA at

relation to a financing that it maintains with that entity.

Therefore, there is no doubt, given the applicable legislation, the lack of measures

organizational or technical measures established by the defendant, and may have determined

a protocol that tells employees that they cannot do it or some mechanism in

the email itself notifying that the email is being sent to several

recipients before it is sent, that prevent the confidentiality of

the data, which in turn entails the infringement 5.1 f) of the RGPD.

It should be noted that the RGPD its article 32 does not establish a list of the

security measures that are applicable according to the data that are subject

of treatment, but 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 the treatment, the risks of probability

and seriousness for the rights and freedoms of the persons concerned.

Likewise, the security measures must be adequate and

proportionate to the detected risk, pointing out that the determination of the measures

technical and organizational information must be carried out taking into account: pseudonymization and

encryption, the ability to ensure the confidentiality, integrity, availability and

resiliency, the ability to restore availability and access to data after a

incident, verification process (not audit), evaluation and assessment of the

effectiveness of the measures.

In any case, when evaluating the adequacy of the level of security,

particularly taking into account the risks presented by the processing of data, such as

consequence of the accidental or unlawful destruction, loss or alteration of data

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data and that could cause damages

physical, material or immaterial.

In this same sense, recital 83 of the RGPD states that:

“(83) In order to maintain security and prevent the treatment from violating the provisions of

this Regulation, the person in charge or the person in charge must evaluate the risks

inherent to the treatment and apply measures to mitigate them, such as encryption. These

measures must ensure an adequate level of security, including the

confidentiality, taking into account the state of the art and the cost of its application

regarding the risks and the nature of the personal data that must be

protect yourself. When assessing the risk in relation to data security,

take into account the risks arising from the processing of personal data,

such as the accidental or unlawful destruction, loss or alteration of personal data

transmitted, stored or otherwise processed, or the communication or access is not

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

IV

Article 72.1.a) of the LOPDGDD states that “according to what is established

Article 83.5 of Regulation (EU) 2016/679 are considered very serious and

Infractions that suppose a substantial violation will prescribe after three years.

of the articles mentioned therein 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

However, article 58.2 of the RGPD provides the following: “Each authority

of control will have all the following corrective powers indicated below:

continuation:

(…)

b) sanction any person responsible or in charge of the treatment with

warning when the processing operations have violated the provisions of

this Regulation;

(…)”

Therefore, the RGPD, without prejudice to the provisions of its article 83, contemplates

in its article 58.2 b) the possibility of going to the warning to correct the

processing of personal data that do not meet your expectations.

According to the available evidence and the

documentation provided shows that the respondent sent the mail

email about the claimant's financial situation to mailboxes that are clearly not

corresponded to the claimant, violating the duty of confidentiality, which

constitutes, on the part of the defendant, two infractions, one against the provisions of the

article 32 of the RGPD and another against the provisions of article 5.1 f) of the RGPD, which governs

the principles of integrity and confidentiality of personal data, as well as the

proactive responsibility of the controller to demonstrate its

compliance.

These offenses are sanctioned with a warning. According to

article 58.2.b) of the RGPD, and considering that the administrative fines that could

fall in accordance with the provisions of article 83.5.b) of the RGPD would constitute a

disproportionate burden for the claimed.

Likewise, for the purposes provided in article 58.2 of the RGPD, the measure

corrective measure that could be imposed on the respondent would consist of requiring him to proceed to

adopt the necessary measures to stop the behavior that is the subject of this claim,

that has caused the reported security breach, so that the effects are corrected

of the infraction committed and its adequacy to the requirements contemplated in article

32 of the RGPD, as well as the provision of accrediting means of compliance with the

required.

Therefore, in accordance with the applicable legislation, the Director of the Agency

Spanish Data Protection RESOLVES:

FIRST: IMPOSE Management and Administration of Receipts S.A. with CIF

A83052621:

□

□

for an infringement of article 32 of the RGPD, typified in article 83.4 a) of the

RGPD a sanction of warning and require you to inform the AEPD

of the measures adopted, within a period of one month, to correct the

effects of the offense committed and its adaptation to the requirements

contemplated in article 32 of the RGPD.

for an infringement of article 5.1 f) of the RGPD, typified in article 83.5 a)

of the RGPD a sanction of warning.

SECOND: NOTIFY this resolution to Management and Administration of Receipts

S.A. with CIF A83052621.

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

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