 File No.: PS/00285/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: On December 11, 2020, it entered the Spanish Agency

of Data Protection (AEPD), written claim presented by D. AAA, in

the one who expresses his disagreement with the reception of an electronic message

sent by the entity EXIPAGO, S.L., in which the payment of a debt of

which the entity ***ENTITY.1 is a creditor. As stated, the message was

sent to 88 recipients without hiding their addresses, which in this way

they would have had access to the email address of the other recipients,

as well as their presumed delinquent status. Along with the claim was not provided

copy of received message.

SECOND: On January 21, 2021, after analyzing the documentation that

was in the file, a resolution is issued by the Director of the AEPD, by which

agrees to reject the claim, as there are no reasonable indications of the existence

of an infringement within the competence of the Spanish Agency for the Protection of

Data.

THIRD: Against the aforementioned resolution, on February 21, 2021, the

The claimant filed an appeal for reversal, providing a copy of the message referred to in

the claim.

FOURTH: On March 22, 2021, the Director of the Spanish Agency for

Data Protection decided to uphold the appeal filed.

FIFTH: The General Subdirectorate for Data Inspection proceeded to carry out

preliminary investigative actions to clarify the facts in

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

control in article 57.1 of Regulation (EU) 2016/679 (General Regulation of

Data Protection, hereinafter RGPD), and in accordance with the provisions of the

Title VII, Chapter I, Second Section, of the LOPDGDD, having knowledge of the

following ends:

"First. -

the claim.

Detail of the causes that have motivated the incident that has originated

(...).

Second. - Detailed description of the procedure followed for the referral of this

type of communications with debtors.

(...).

Third. -

Possible succession of other similar incidents.

(...).

Quarter. - Actions taken in order to minimize the adverse effects of this

incident and on the measures adopted for its final resolution.

(...).

Fifth. -

affected.

(...).

Information about the notification of the security breach to the

Sixth. -

Technical and organizational measures adopted.

(...).

Seventh. - Contract for the provision of services signed with the person in charge of the

treatment.

(...).

Eighth. -

Communication of the breach to the data controller.

(...).

SIXTH: On September 1, 2021, the Director of the Spanish Agency for

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

for the alleged infringement of article 5.1.f) of the RGPD and article 32 of the RGPD,

typified in article 83.5 and 83.4 of the RGPD, respectively.

SEVENTH: Once the initiation agreement was notified, the respondent submitted a written

allegations in which, in summary, it stated that the cause that led to the incidence

was a human error in sending an electronic communication, that the methodology

for sending electronic communications to debtors is based on the

need to blind copy (BCC) all recipients, which

employees at the time of joining the company and prior to

performance of their duties receive training in this regard, which proceeded from

immediately notify the data controller of the security breach, that said

employee was reprimanded, that preventive measures have been taken to avoid this

type of incidents in the future and requests that a warning sanction be proposed.

EIGHTH: On December 3, 2021, a resolution proposal was formulated,

proposing:

<<That the Director of the Spanish Agency for Data Protection directs a

warning to EXIPAGO, S.L., with CIF B65984262, for a violation of article

5.1. f) of the RGPD, in accordance with the provisions of article 83.5 of the RGPD, qualified

as very serious for prescription purposes in article 72.1 i) of the LOPDGDD and

an infringement of article 32 of the RGPD, in accordance with the provisions of article 83.4 of the

cited RGPD, qualified as serious for prescription purposes in article 73

section f) of the LOPDGDD >>

NINTH: On December 10, 2021, the respondent files a written document in

which, in short, states that it agrees with the aforementioned Proposal for

Resolution.

In view of everything that has been done, by the Spanish Data Protection Agency

In this proceeding, the following are considered proven facts:

FACTS

FIRST: On December 11, 2020, the claimant filed a written

claim before the Spanish Data Protection Agency (AEPD), in which

expressed his disagreement with the receipt of an email sent by

the claimed entity, in which the payment of a debt was demanded. The message was

sent to 88 recipients without hiding their addresses, having access to the address

e-mail of the other recipients, as well as their presumed condition of

delinquent

SECOND: Checking the documentation provided and that it is incorporated

to the file, it is recorded that on December 11, 2020, at 2:56 p.m., the

claimant received email from the address: ***EMAIL.1, on behalf of

EXIPAGO, S.L., without a blind copy, along with 88 other email addresses,

among which was the address of the claimant and through which it was claimed

a debt that had to be paid or legal action would be taken.

THIRD: The claimed party acknowledges that the incident that is the subject of the claim was

due to human error and states that it has proceeded to implement the measures

adequate corrective actions to avoid the repetition of similar events in the future.

FOUNDATIONS OF LAW

FIRST: In accordance with the powers that article 58.2 of the Regulation (EU)

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

each control authority and as established in articles 47 and 48.1 of the Law

Organic 3/2018, of December 5, on the Protection of Personal Data and guarantee of

digital rights (hereinafter, LOPDGDD), is competent to initiate and resolve

this procedure the Director of the Spanish Data Protection Agency.

Likewise, article 63.2 of the LOPDGDD determines that: “The procedures

processed by the Spanish Agency for Data Protection will be governed by the provisions

in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures.”

SECOND: The facts proven in the procedure evidence the disclosure of the

email addresses when an email is sent to the claimant

without hidden copy with violation of the technical and organizational measures and

violating the confidentiality of the data.

In the present case, the defendant is charged with the infraction of article 5.1.f) and 32.1 of the

RGPD, typified in articles 83.5.a) and 83.4.a) of the RGPD.

THIRD: Article 5 of the RGPD, Principles related to treatment, which establishes

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").

(…)"

Article 5, Duty of confidentiality, of the new Organic Law 3/2018, of 5

December, Protection of Personal Data and Guarantee of Digital Rights

(hereinafter LOPDGDD), states that:

"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".

The documentation in the file offers clear indications that the

claimed violated article 5 of the RGPD, principles related to treatment, in

relation to article 5 of the LOPGDD, duty of confidentiality, when disclosing to

third parties, personal data, when sending without a blind copy a claim of

debt.

This duty of confidentiality, previously the duty of secrecy, must be understood

whose purpose is to prevent leaks of data without consent

by their owners.

Therefore, this duty of confidentiality is an obligation that falls not only on the

responsible and in charge of the treatment but to anyone who intervenes in any

phase of the treatment and complementary to the duty of professional secrecy.

FOURTH: Article 32 of the RGPD, security of treatment, establishes the following:

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

of the 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 (The underlining is from the AEPD).

Recital 75 of the RGPD lists a series of factors or assumptions associated with

risks for the guarantees of the rights and freedoms of the interested parties:

“The risks to the rights and freedoms of natural persons, serious and

variable probability, may be due to the processing of data that could cause

physical, material or non-material damages, particularly in cases where

that the treatment may give rise to problems of discrimination, usurpation of

identity or fraud, financial loss, reputational damage, loss of

confidentiality of data subject to professional secrecy, unauthorized reversal of the

pseudonymization or any other significant economic or social damage; in the

cases in which the interested parties are deprived of their rights and freedoms or are

prevent exercising control over your personal data; In cases where the data

treated personalities reveal ethnic or racial origin, political opinions, religion

or philosophical beliefs, militancy in trade unions and the processing of genetic data,

data relating to health or data on sex life, or convictions and offenses

criminal or related security measures; In cases where they are evaluated

personal aspects, in particular the analysis or prediction of aspects related to the

performance at work, economic situation, health, preferences or interests

personal, reliability or behavior, situation or movements, in order to create or use personal profiles; in the cases in which personal data of vulnerable people, in particular children; or in cases where the treatment involves a large amount of personal data and affects a large number of interested."

FIFTH: Article 4.12 of the RGPD establishes that it is considered “violation of the security of personal data: any breach of security that causes the accidental or unlawful destruction, loss or alteration of transmitted personal data, stored or otherwise processed, or unauthorized communication or access to said data.”

From the documentation in the file, there are clear indications that the claimed has violated article 32 of the RGPD, when there was a breach of security, by sending an email without a blind copy to 88 recipients, among them the claimant, in which a debt was claimed, revealing information and data of a personal nature to third parties.

It should be noted that the RGPD in the aforementioned precept 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 technical measures and organizational must be carried out taking into account: pseudonymization and encryption, capacity to guarantee 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 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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

SIXTH: The infringement is typified in article 83.5 of the RGPD, which provides the

Next:

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

paragraph 2, with administrative fines of a maximum of EUR 20,000,000 or,

in the case of a company, an amount equivalent to a maximum of 4% of the

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

the largest amount:

a)

basic principles for treatment, including conditions for con-

sentiment under articles 5, 6, 7 and 9;”

For its part, article 71 of the LOPDGDD, under the heading "Infringements" determines what

following: "The acts and behaviors referred to in the

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law.”

For the purposes of the limitation period for infractions, article 72 of the LOPDGDD,

under the rubric of infractions considered very serious, it establishes the following: “1. In

Based on the provisions of article 83.5 of Regulation (EU) 2016/679,

considered very serious and will prescribe after three years the infractions that suppose

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

following:

(…)

Yo)

The violation of the duty of confidentiality established in article 5 of

this organic law.

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

cited RGPD in the following terms:

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

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 in accordance with articles 8, 11,

25 to 39, 42 and 43.”

(…)

For the purposes of the limitation period for infractions, article 73 of the LOPDGDD,

under the heading "Infringements considered serious", it establishes the following:

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

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:

(…)

f) The lack of adoption of those technical and organizational measures that result

appropriate to guarantee a level of security appropriate to the risk of the treatment,

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

In the present case, the infringing circumstances provided for in article

83.5 and 83.4 of the GDPR.

SEVENTH: Establishes Law 40/2015, of October 1, on the Legal Regime of the Sector

Public, in Chapter III on the "Principles of the power to sanction", in the

Article 28 under the heading "Responsibility", the following:

"1. They may only be sanctioned for acts constituting an administrative infraction.

natural and legal persons, as well as, when a Law recognizes their capacity to

to act, the affected groups, the unions and entities without legal personality and the

independent or autonomous estates, which are responsible for them

title of fraud or guilt."

Lack of diligence in implementing appropriate security measures

with the consequence of breaching the principle of confidentiality constitutes the

element of guilt.

EIGHTH: Without prejudice to the provisions of article 83.5 sections a) and b) of the

RGPD, in its art. 58.2 b) provides for the possibility of directing a warning, in relation to

with what is stated in Considering 148:

"In the event of a minor offence, or if the fine likely to be imposed

would constitute a disproportionate burden for a natural person, rather than

sanction by means of a fine, a warning may be imposed. must however

Special attention should be paid to the nature, seriousness and duration of the infringement, its

intentional nature, to the measures taken to alleviate the damages suffered,

the degree of liability or any relevant prior violation, the manner in which

that the control authority has been aware of the infraction, compliance

of measures ordered against the person responsible or in charge, adherence to codes of

conduct and any other aggravating or mitigating circumstance."

In the present case, based on the diligence carried out by the entity

claimed in relation to informing this Agency of the circumstances in which

the incident that gave rise to the claim occurred, as well as the measures to be adopted

in order to prevent events such as the one claimed from occurring again in the future,

considering that the answer has been reasonable, acknowledging the facts and, not

having evidence of other claims by the affected persons,

allows to consider a reduction of guilt in the facts, for which it is considered

in accordance with the law, not to impose a sanction consisting of an administrative fine and

replace it with a warning, in accordance with article 76.3 of the LOPDGDD,

in relation to article 58.2 b) of the RGPD that states the following:

2. Each control authority will have all of the following corrective powers in-

listed below:

(…)

“b) send a warning to any person responsible or in charge of the treatment when

treatment operations have infringed the provisions of these Regulations.

unto.”

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of the sanctions whose existence has been proven, the Director of the

Spanish Data Protection Agency RESOLVES:

FIRST: ADDRESS EXIPAGO, S.L., with CIF B65984262, for an infraction of the

article 5.1.f) of the RGPD and article 32 of the RGPD, typified in article 83.5 and 83.4 of the

GDPR, respectively, a warning.

SECOND: NOTIFY this resolution to EXIPAGO, 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 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 month from

counting 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,

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 by

writing addressed to the Spanish Agency for Data Protection, presenting it through

Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registers provided for in art. 16.4 of the

aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the

documentation proving the effective filing of the contentious appeal-

administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative within a period of two months from the day following the

notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-270122

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es