 Procedure No.: PS/00328/2021

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 March 11, 2020

filed a claim with the Spanish Data Protection Agency. The

B.B.B., with NIF ***NIF.1 (PISAMUNDO

claim is directed against Ms.

ZARAGOZA) (hereinafter, the claimed party).

The claimant states that on January 30, 2020 he received an email without

blind copy revealing others' email addresses

recipients.

And, provide the following documentation:

- Email where four recipients appear without hiding.

SECOND: Prior to the acceptance of this claim for processing, it is

transferred the claimed person on June 1, 2020, in accordance with the provisions of

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

Personal and guarantee of digital rights (hereinafter, LOPDGDD), in the

actions with reference E/03555/2020. Notification is done electronically,

and figure returned to origin because the shipment was not picked up from the post office on June 18

of 2020.

Subsequently, it was repeated on the 23rd of the same month and year, with the same result, with

date July 9, 2020.

THIRD: In accordance with the provisions of article 65.2 of the Organic Law

3/2018, on Data Protection and Guarantee of Digital Rights (LOPDGDD), in

On September 29, 2020, the agreement for admission to processing of the application was signed.

claim.

FOURTH: 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 Organic Law 3/2018, of December 5,

Protection of Personal Data and guarantee of digital rights (hereinafter

LOPDGDD).

1. On the web page of the website www.pisamundo.com, they indicate as responsible for the

site to Donosti Receptivo, S.L. According to a report from the Axesor database, this

entity belongs to the mercantile Departamento Infraestructuras Turísticas, S.L. (in

forward, Dit Management).

2. Information request made to Dit Management to clarify the relationship of

this merchant with the claimed travel agency. Dated October 26,

2020 is received in this Agency, written of allegations showing that

PISAMUNDO ZARAGOZA is a trade name that belongs to Ms. B.B.B.

as stated in the database of the Spanish Patent and Trademark Office.

They add that their company has no connection with said distinctive sign and in

Consequently, they do not have and have not had any contractual relationship with their legitimate owner, understanding consequently that if someone is responsible for the treatment of personal data corresponding to said commercial name will be the owner of it. They clarify that Dit Gestión is the owner of the trade name "PISAMUNDO", the only commercial name assigned in use to Ms. B.B.B. Through the Contract of service.

Attach the following documents:

- Service provision contract. In this contract, the use of the trade name "PISAMUNDO" under certain commercial conditions in the that the agency of Ms. B.B.B. as interested in the sale of travel services as an independent agent in Zaragoza.
- Agreement to regulate the processing of personal data. in this agreement DIT Management holds the status of person in charge of processing the data of personal character necessary to provide the services described in the contract of collaboration formalized between Dit Gestión and Ms. B.B.B..

3. Request made for information on the entity responsible for the agency of trips "PISAMUNDO ZARAGOZA" to Ms. B.B.B., notified on February 3 of 2021.

The respondent has not responded to the information request that was sent.

FIFTH: On July 19, 2021, the Director of the Spanish Agency for Data Protection agreed to initiate a sanctioning procedure against the claimed party, for the alleged infringements of articles 5.1f) and 32 of the RGPD, typified in the articles 83.5 a) and 83.4 a) of the RGPD respectively. This agreement was notified to through the public postal operator and the single edictal board of the BOE on July 29 and 9 August 2021, to the claimed party.

SIXTH: Formal notification of the initiation agreement, the claimed party at the time of

this resolution has not submitted a brief of arguments, so it is

application of what is stated in article 64 of Law 39/2015, of October 1, of the

Common Administrative Procedure of Public Administrations, which in its

section f) establishes that in the event of not making allegations within the stipulated period

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.

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 March 11, 2020, the complaining party states that on March 30

January 2020 received an unblinded email disclosing the

email addresses of the other recipients.

SECOND: The complaining party provides a copy of the email where they appear

four unhidden recipients.

THIRD: In the public database of the Spanish Patent and Trademark Office,

It is known that PISAMUNDO Zaragoza is a commercial name that belongs to Ms.

B.B.B., with filing date on August 11, 2016 and still in force.

FOURTH: The sender of the email is info.pisamundozaragoza.com, name

of the entity and whose responsible owner is Ms. B.B.B..

FIFTH: On July 19, 2021, this sanctioning procedure was initiated by the

alleged infringement of article 6 of the RGPD, being notified on August 9, 2021.

Not having made allegations, the claimed party, to the initial agreement.

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 LOPDPGDD, the

Director of the Spanish Data Protection Agency is competent to resolve

this procedure.

II

The defendant is charged with the commission of two infractions for 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 the 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 by sending an email without a blind copy to four

recipients, claimant included.

It should be noted that the RGPD in the aforementioned provision does not establish a list of

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

object of treatment, but it establishes that the person in charge and the person in charge of the

treatment will apply technical and organizational measures that are appropriate to the risk

that the treatment entails, taking into account the state of the art, the costs of

application, 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

provided in 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 guarantee an adequate level of security, including

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) direct any person responsible or in charge of the treatment with a warning

when the treatment 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

The documentation provided shows that from the facts denounced, that is,

sending an email without a blind copy, sent to other recipients, supposes the

violation 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

responsible for the treatment to demonstrate its compliance, which constitutes, by

part of the claimed, of two infractions, one against the provisions of article 32 of the

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

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

proactive of the data controller to demonstrate 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

load disproportionate to that claimed.

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

corrective measure imposed on the respondent party consists of requiring him to take

adequate security measures so that when you send emails to different

recipients use the option to send with a blind copy to avoid giving

information with personal data to all recipients.

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 Ms. B.B.B., with NIF ***NIF.1 (PISAMUNDO ZARAGOZA), two

warnings:

□

□

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

GDPR a warning.

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

GDPR a warning.

SECOND: REQUEST Ms. B.B.B., with NIF ***NIF.1 (PISAMUNDO ZARAGOZA),

so that within one month from the notification of this resolution, prove:

-

The security measures taken to prevent when they are sent

mailings to different recipients use the blind copy sending option

to avoid transferring personal data information to all recipients of the

mail.

THIRD: NOTIFY this resolution to Ms. B.B.B., with NIF ***NIF.1

(PISAMUNDO ZARAGOZA).

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

938-300320

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es