 Procedure No.: PS/00288/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant) dated May 29, 2020

filed a claim with the Spanish Data Protection Agency.

The claim is directed against PRAKMA INNOVATION, S.L. with NIF B67088419 (in

later, the claimed one).

The reasons on which the claim is based are that the claimed party sends an email

email without a blind copy, to eight recipients, including the claimant, to whom

reports the blocking of your accounts.

A copy of the message is provided.

SECOND: The present claim was transferred to the respondent on July 3, 2020,

requiring him to send to this Agency, within a period of one month, information

about the response given to the claimant for the facts denounced, as well as the

causes that have motivated the incident and the measures adopted, but the entity

claimed has not answered within the period indicated.

THIRD: On January 14, 2021, the Director of the Spanish Agency for

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

alleged violations one of article 5.1.f) and another of article 32.1 of the RGPD,

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

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: The respondent sends an email without a blind copy, to eight

recipients, including the claimant.

SECOND: On January 26, 2021, the agreement to start this

procedure, becoming the same in resolution proposal in accordance

with articles 64.2.f) and 85 of Law 39/2015, of October 1, on Procedure

Common Administrative System of Public Administrations (LPACAP), by not carrying out

claims within the specified period.

FOUNDATIONS OF LAW

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

control, and according to the provisions of articles 47 and 48 of the LOPDGDD, the Director

of the Spanish Agency for Data Protection is competent to initiate and to

resolve this procedure.

Yo

Article 58 of the GDPR states:

II

"two. Each supervisory authority will have all of the following corrective powers

listed below:

(…)

i) impose an administrative fine under article 83, in addition to or instead of

the measures mentioned in this section, according to the circumstances of each

particular case;

(…)”

The RGPD establishes in article 5 of 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) processed in such a way as to ensure adequate security of the data

including protection against unauthorized or unlawful processing and against

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

or appropriate organizational ("integrity and confidentiality").

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

RGPD, where it is established 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;

the ability to ensure the confidentiality, integrity, availability and

a)

permanent resilience of treatment systems and services;

the ability to restore availability and access to personal data

b)

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and assessment 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 account shall be taken of

takes 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 person in charge or the person in charge and

has access to personal data can only process said data following

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

the Union or the Member States.

The violation of article 32.1 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 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 of the person in charge pursuant to articles 8, 11, 25 a

39, 42 and 43.

(…)”

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

infractions the acts and behaviors referred to in sections 4, 5 and 6 of the

Article 83 of Regulation (EU) 2016/679, as well as those that are contrary to the

present 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,

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 breach, as a consequence of the lack of due diligence, of the

technical and organizational measures that have been implemented as required

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

III

The GDPR defines personal data security breaches as “all

those breaches 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, it is verified that the respondent has

violated article 32.1 of the RGPD, when a security breach occurred in its

systems when sending an email without a blind copy, to eight recipients, among

them the claimant, to whom he informs of the blocking of their accounts.

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.

IV

In this claim, it is reported that the respondent sends an email without blind copying, to eight recipients, which implies the lack of adoption of measures appropriate technical and organizational measures to guarantee an adequate level of security, by the claimed party, informing the recipients of the mail without blind copy of the address of others.

Therefore, such facts violate the data protection regulations of

in accordance with the provisions of article 5.1 f) and article 32.1 of the RGPD.

v

Article 72.1 a) of the LOPDGDD states that “according to what is established in the article 83.5 of Regulation (EU) 2016/679 are 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:

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

Article 73.1.f) of the LOPDGDD states that “according to what is established in the Article 83.4 of Regulation (EU) 2016/679 are considered serious and will prescribe the 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.”

SAW

Article 58.2 of the RGPD provides the following: "Each control authority will have of all the following corrective powers indicated below:

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

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

i) impose an administrative fine under article 83, in addition to or instead of the

measures mentioned in this section, according to the circumstances of each case

particular;

Article 83.5 of the RGPD establishes that infractions that affect

a:

“a) the basic principles for the treatment, including the conditions for the

consent under articles 5, 6, 7 and 9;

b) the rights of the interested parties pursuant to articles 12 to 22.”

Article 83.4 of the RGPD establishes that infractions that affect

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.”

7th

Among the corrective powers contemplated in article 58 of the RGPD, in its section 2

d) it is established that each control authority may “order the person in charge or

in charge of the treatment that the treatment operations comply with the

provisions of this Regulation, where appropriate, in a certain way

and within a specified period…”. The imposition of this measure is compatible with

the sanction consisting of an administrative fine, as provided in art. 83.2 of the

GDPR.

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

graduation of sanctions whose existence has been proven,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE PRAKMA INNOVATION, S.L., with NIF B67088419, for a

infringement of article 32 of the RGPD, and another of article 5.1.f) of the RGPD, typified in the

article 83.5 of the RGPD, with a sanction of warning.

SECOND: ORDER that the appropriate measures be adopted so that

the infringing conduct ceases, the effects of the infractions that have occurred are corrected

committed, adopting the necessary measures so that the defendant acts in accordance with

in accordance with the principles of "integrity and confidentiality" of art. 5.1 f) of

RGPD and is adapted to the requirements contemplated in article 32.1 of the RGPD, as well as

as the provision of means accrediting compliance with what is required.

THIRD: NOTIFY this resolution to PRAKMA INNOVATION, 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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es