 File No.: PS/00084/2021

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 complaining party) dated October 16, 2020

filed a claim with the Spanish Data Protection Agency. The

claim is directed against AURORA ENERGY SUPPLY S.L. with CIF B17657719

(hereinafter AURORA) The reasons on which the claim is based are the following:

“Yesterday, October 15, I received 160 emails from the ASICXXI company, to which

my electric company Aurora Energy Supply has contracted as a provider of

computer services of the company. These emails were addressed to all

customers, and in these mails you can read the email addresses of

clients, including mine, revealing everyone's private information

the clients"

Along with the claim, provide a copy of one of the emails in which

The email addresses of a plurality of customers are listed.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

December, of Protection of Personal Data and guarantee of digital rights (in

hereinafter LOPDGDD), said claim was transferred to AURORA so that

proceed to its analysis and inform this Agency within a month of the

actions carried out to adapt to the requirements set forth in the regulations of

Data Protection.

On 01/12/2021, this Agency received a written response indicating:

-On 10/15/2020 they detected an attempt to scam their clients, by means of a call

phone, threatening to cut off the electricity supply if they did not give up their data

personal and banking

-Given this fact, they decided to contact their clients by email,

which was sent to the company ASIC XXI S.L., with CIF B99276917, (hereinafter,

ASIC), a company with which they have a computer services contract, being one of

them sending communications to customers. On 10/15/2021, ASIC proceeded to

sending the email making the mistake of not blind copying the

recipients, causing the sending of a mass mail.

-On 10/16/2021, ASIC sends an email to AURORA communicating the error

committed and assuming its responsibility.

THIRD: On January 16, 2021, the application was admitted for processing.

claim filed by the claimant.

FOURTH: On December 2, 2021, the Director of the Spanish Agency for

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

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

83.5 of the GDPR.

FIFTH: On January 13, 2022, a resolution proposal was formulated,

proposing that the Director of the Spanish Data Protection Agency

sanction ASIC XXI, S.L., with CIF B99276917, with a WARNING for a

infringement of Article 5.1.f) of the RGPD, typified in Article 83.5 of the RGPD, and with

a WARNING for an infringement of Article 32 of the RGPD, typified in the

article 83.4 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:

PROVEN FACTS

FIRST: It is proven that ASIC sent an email to clients of

AURORA ENERGY SUPPLY S.L., making the mistake of not blind copying

recipients, causing the sending of a mass email.

SECOND: It is proven, according to ASIC, that this fact was due to a

isolated error, and that measures have been taken to prevent it from returning

to occur in the future.

FOUNDATIONS OF LAW

Yo

In accordance with the powers that article 58.2 of 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.”

In the present case, in accordance with the provisions of article 4.1 of the RGPD, it consists

carrying out personal data processing, since ASIC performs, among

II

other treatments, the use of the following personal data of people

physical, such as: name, email address, etc. ASIC does this

activity in its capacity as data processor, given that it processes this data

on behalf of AURORA ENERGY SUPPLY S.L., which is responsible for

this treatment in question, all under article 4.8 of the RGPD.

ASIC is accused of committing an infraction for violation of article 5.1.f) of the

RGPD, and for violation of article 32 of the RGPD.

III

Article 5.1.f) “Principles related to treatment” of the RGPD establishes:

"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").

The aforementioned infringement of article 5.1.f) of the RGPD could lead to the commission of the

offenses typified in article 83.5 of the RGPD that under the heading "Conditions

rules for the imposition of administrative fines” provides:

“Infractions of the following provisions will be sanctioned, in accordance

with paragraph 2, with administrative fines of EUR 20,000,000 as

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

as a maximum of the overall annual total turnover of the financial year

above, opting for the highest amount:

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

consent under articles 5, 6, 7 and 9; (…)”

In this regard, the LOPDGDD, in its article 71 "Infringements" establishes that:

“The acts and behaviors referred to in the regulations constitute infractions.

paragraphs 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as the

that are contrary to this organic law.

For the purposes of the statute of limitations, article 72 “Infringements considered

very serious” of the LOPDGDD indicates:

"1. Based on the provisions of article 83.5 of the 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:

The processing of personal data violating the principles and guarantees established

in article 5 of Regulation (EU) 2016/679. (…)”

Since it has been shown throughout the procedural instruction that ASIC has

disseminated personal data of the complaining party and 160 other people, without their

consent, by sending at least, according to the documentation in the file,

mass email without blind copying, thus allowing each of the

recipients had access to the email address of the rest, it is

accredited the infringement of article 5.1.f) of the RGPD.

Without prejudice to the provisions of article 83 of the RGPD, the aforementioned Regulation provides

in section 2.b) of article 58 "Powers" the following:

IV

“Each supervisory authority shall have all of the following corrective powers

listed below:

(…)

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

when the treatment operations have infringed the provisions of the

this Regulation; (…)”

For its part, recital 148 of the RGPD indicates:

“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.”

Article 32 “Security of treatment” of the RGPD establishes:

v

"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 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 aforementioned infringement of article 32 of the RGPD could lead to the commission of the

offenses typified in article 83.4 of the RGPD, which under the heading "Conditions

rules for the imposition of administrative fines" provides:

"The infractions of the following dispositions 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 pursuant to articles 8,

11, 25 to 39, 42 and 43; (…)"

In this regard, the LOPDGDD, in its article 71 "Infringements" establishes 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.

For the purposes of the limitation period, article 73 "Infringements considered serious"

of the LOPDGDD indicates:

"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

are appropriate to guarantee a level of security appropriate to the risk

of the treatment, in the terms required by article 32.1 of the Regulation

(EU) 2016/679.

From the instruction carried out in this procedure, it is considered that ASIC

has breached the provisions of article 32 of the RGPD, by not having the measures

appropriate organizational and technical measures to prevent the sending of an email without

hidden copy. It is, therefore, accredited, the infringement of the aforementioned article.

SAW

Without prejudice to the provisions of article 83 of the RGPD, the aforementioned Regulation provides

in section 2.b) of article 58 "Powers" the following:

“Each supervisory authority shall have all of the following corrective powers

listed below:

(…)

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

when the treatment operations have infringed the provisions of the

this Regulation; (…)”

For its part, recital 148 of the RGPD indicates:

“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."

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:

7th

FIRST: Direct ASIC XXI, S.L., with CIF B99276917, for an infringement of the

Article 5.1.f) of the RGPD, typified in Article 83.5 of the RGPD, a warning.

Address ASIC XXI, S.L., with CIF B99276917, for an infraction of Article 32 of the

RGPD, typified in Article 83.4 of the RGPD, a warning.

SECOND: NOTIFY this resolution to ASIC XXI, 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