 Procedure No.: PS/00354/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: The SEPRONA Section of LAS PALMAS dated 06/18/2020

filed a claim with the Spanish Data Protection Agency. The

claim is directed against D. A.A.A. with NIF ***NIF.1 (hereinafter, the claimed one).

The reasons on which the claim is based are: that on 03/13/2020, the SEPRONA section

of the GC of Las Palmas found next to some urban garbage containers

located at the entrance of the neighborhood of ***BARRIADA.1 in ***LOCALIDAD.1 (Great

Canaria) two plastic bags full of documentation, in which data appears

personal data from different clients of the defendant, a lawyer by profession.

That among the documentation are deeds, powers of attorney, judgments

of judicial bodies, photocopies of DNIs of clients, wills and other documents

with personal data. The GC has tried to contact the respondent but has not

achieved since he does not answer calls.

SECOND: Upon receipt of the claim, the Subdirectorate General for

Data Inspection proceeded to carry out the following actions:

On 07/06/2020, the claim submitted was transferred to the defendant for analysis

and communication to the claimant of the decision adopted in this regard. Likewise, it

required so that within a month it would send to the Agency determined

information:

- Copy of the communications, of the adopted decision that has been sent to the

claimant regarding the transfer of this claim, and proof that

the claimant has received communication of that decision.

- Report on the causes that have motivated the incidence that has originated the

claim.

- Report on the measures adopted to prevent the occurrence of

similar incidents.

- Any other that you consider relevant.

There is no response from the respondent to the request for information from the AEPD.

THIRD: On 08/26/2020, in accordance with article 65 of the LOPDGDD, the

Director of the Spanish Agency for Data Protection agreed to admit for processing the

claim filed by the claimant against the respondent.

FOURTH: On 11/05/2020, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged

infringement of article m32.1 of the RGPD, considering that the sanction that could

to correspond would be a WARNING.

FIFTH: 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.

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

accredited the following:

PROVEN FACTS

FIRST: On 06/18/2020, the SEPRONA Section of LAS PALMAS sent to the

Spanish Agency for Data Protection Act Complaint/Inspection and Request for

start of procedure nº ***PROCEDURE.1 for infringement of the regulations on

Personal data protection; on 03/13/2020, the SEPRONA section of the

GC of Las Palmas found next to some urban garbage containers located

the entrance of the neighborhood of ***BARRIADA.1 in ***LOCALIDAD.1 (Gran Canaria) two

plastic bags full of documentation, in which personal data of

different clients of the defendant, a lawyer by profession; enter the documentation

found are deeds, powers of attorney, judgments of judicial bodies,

photocopies of DNIs of clients, wills and other documents with personal data;

some of the documents found in the bags are described; the civil Guard

I try to contact the claimed person but he has not been able to since he does not answer the

calls.

SECOND: They include a photographic report of the documentation located as follows:

as photographs of some of the documents outlined above in which

personal data of the claimed clients are included.

FOUNDATIONS OF LAW

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

control authority, 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 solve this procedure.

Yo

Article 58 of the RGPD, Powers, states:

II

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

corrections listed below:

(…)

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

warning when the treatment operations have infringed the

provided in this Regulation;

(…)”

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

of personal data, 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 processing or

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 articles

32, 33 and 34 of the RGPD.

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".

Violations of article 32 are 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 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

to what is required by article 32.1 of Regulation (EU) 2016/679”.

(…)

The facts revealed in this claim are specified in

the existence of a security incident in the claimed systems allowing

the vulnerability of the same by allowing documentation containing data from

personal character, were located next to some urban garbage containers

located in a neighborhood belonging to ***LOCALIDAD.1 (Gran Canaria) in bags of

plastic, from different clients of the claimed one, allowing access to the data

contained in them.

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”.

III

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

that the claimed party has violated article 32.1 of the RGPD, when there was a breach of

security in their systems allowing access to the documents contained in

bags deposited next to some urban garbage containers located in

***LOCATION.1; documents containing personal data of clients of the

reclaimed.

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.

In the present case, as evidenced by the facts and within the framework of the

investigation file E/05538/2020, the AEPD transferred the defendant on

07/06/2020 the written claim submitted for analysis requesting the

provision of information related to the claimed incidence, without

received any response from this body.

The responsibility of the claimed party is determined by the incident/bankruptcy

of security revealed by the SEPRONA section of the GC of Las

Palmas, since it is responsible for making decisions aimed at implementing

effectively the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk to ensure the confidentiality of the data, restoring their availability and preventing access to them in the event of an incident physical or technical. However, the documentation provided shows that the claimed has not only failed to comply with this obligation, but also the adoption of measures in this regard, despite having notified him of the claim presented.

In accordance with the foregoing, it is estimated that the respondent would be allegedly responsible for the infringement of the RGPD: the violation of article 32.1, infraction typified in its article 83.4.a).

IV

However, as stated in Foundation II, article 58.2 of the RGPD provides the following: "Each control authority will have all the following corrective powers indicated below:

(…)

b) sanction any person responsible or in charge of the treatment with warning when the treatment operations have infringed the provided in 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.

In the case at hand, it has been proven that the defendant

violated article 32.1 of the RGPD, by allowing third parties to have access to the

data contained in the documents that had been deposited with

existing garbage containers on the public road at the entrance of the neighborhood of

***BARRIADA.1, belonging to the municipality of ***LOCALIDAD.1; documents that

they contained personal data of clients of the claimed party.

According to the available evidence, said conduct

constitutes, on the part of the defendant, the infringement of the provisions of article 32.1 of the

GDPR.

This infringement in accordance with article 58.2.b) of the RGPD can be

sanctioned with a warning considering that the administrative fine that could

fall in accordance with the provisions of article 83.4.a) of the RGPD would constitute a

disproportionate burden for the defendant, in addition to the fact that the commission of

no previous breach of data protection.

In addition, in accordance with article 58.2 of the RGPD, the

requested to adopt adequate technical measures to ensure the

confidentiality of the information included in their systems so that in the future they do not

may incur in incidents such as the one that has given rise to this file, as well as

such as the provision of means of proof accrediting compliance with the

required.

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 D. A.A.A., with NIF ***NIF.1, for an infraction of the

aarticle 32.1 of the RGPD, typified in Article 83.4.a) of the RGPD, a sanction of

warning.

SECOND: REQUEST D. A.A.A., with NIF ***NIF.1, so that within the period of

one month from the notification of this resolution, accredit before the AEPD the adoption of

the necessary and pertinent measures to correct data processing

personal data that do not comply with the data protection regulations of

personal nature and prevent the recurrence of violations such as those that have

given rise to the claim correcting the effects of the infringement, determining the

necessary measures in order to adapt to the requirements contemplated in the

article 32.1 of the RGPD.

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

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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es