Procedure No.: PS/00464/2020

 RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: The FORAL POLICE OF NAVARRA (hereinafter, the claimant) on the date

08/07/2020 sent a complaint bulletin to the Spanish Agency for the Protection of

Data. The claim is directed against KUKIMBIA S.L., with NIF B99352023 (in

later, the claimed one). The grounds on which the claim is based are that it has

found abandoned documentation containing personal data,

from a company that abandoned a ship adjacent to the area in which

said documentation has been found abandoned.

Photographs are provided with the abandoned material.

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

Data Inspection proceeded to carry out the following actions:

On 09/28/2020, 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 12/09/2020, 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 02/12/20210, the Director of the Spanish Protection Agency

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

infringement of article 32.1 of the RGPD, typified in article 83.4.a) of the aforementioned

Regulation, and considered for prescription purposes as a serious infringement in the

Article 73.g) of the LOPDGDD, a penalty of 3,000 euros.

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 08/07/2020 you have an entry in the AEPD police complaint bulletin FORAL DE NAVARRA (hereinafter, the claimant), stating the abandonment of documentation of clients and suppliers of the claimed, containing data of personal character, next to a garbage container and access by third parties.

SECOND: The defendant is a company incorporated in Zaragoza on 08/03/2012 and its corporate purpose is the storage, distribution and transportation throughout the national territory and abroad of all kinds of goods.

THIRD: Report No. 01132421 of the Navarra Provincial Police has been provided, matter spilled of documentation in the Ezkarbarte de Arre industrial estate, pointing out that their passage through the aforementioned polygon they observed the existence of documentation abandoned containing personal data of carriers and customers (name and surnames, ID number, telephone number) from the company ***COMPANY.1 located in the city of transportation in ***LOCATION.1, ***ADDRESS.1; who headed to the company, although they verified that they no longer operated in the area, having ceased their activity in the ship they had rented; however, they tried to contact the said company; On 06/16/2020 they received the following response from it:

Hello,

In response to the photos received

On XX/YY/2020 we evacuated the facilities of ***EMPRESA.2.

Removing merchandise and office supplies and "files we could."

At that time we no longer had access or keys to the facilities.

FOURTH: Photographs of the abandoned documentation are provided: letters, delivery notes, etc., containing data of a personal nature.

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,

Yo

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/10

The Director of the Spanish Agency for Data Protection is competent to initiate

and to solve this procedure.

Law 39/2015, of October 1, on the Common Administrative Procedure of

the Public Administrations, in its article 64 "Agreement of initiation in the

procedures of a sanctioning nature", provides:

II

"1. The initiation agreement will be communicated to the instructor of the procedure, with

transfer of how many actions exist in this regard, and the interested parties will be notified,

understanding in any case by such the accused.

Likewise, the initiation will be communicated to the complainant when the regulatory norms

of the procedure so provide.

2. The initiation agreement must contain at least:

a) Identification of the person or persons allegedly responsible.

b) The facts that motivate the initiation of the procedure, its possible

rating and sanctions that may apply, without prejudice to what

result of the instruction.

c) Identification of the instructor and, where appropriate, Secretary of the procedure, with

express indication of the system of recusal of the same.

d) Competent body for the resolution of the procedure and regulation that

attribute such competence, indicating the possibility that the presumed

responsible can voluntarily acknowledge their responsibility, with the

effects provided for in article 85.

e) Provisional measures that have been agreed by the body

competent to initiate the sanctioning procedure, without prejudice to those that

may be adopted during the same in accordance with article 56.

f) Indication of the right to formulate allegations and to the hearing in the

procedure and the deadlines for its exercise, as well as an indication that, in

If you do not make allegations within the stipulated period on the content of the

initiation agreement, this may be considered a resolution proposal

when it contains a precise statement about the responsibility

imputed.

3. Exceptionally, when at the time of issuing the initiation agreement

there are not sufficient elements for the initial qualification of the facts that motivate

the initiation of the procedure, the aforementioned qualification may be carried out in a phase

later by drawing up a List of Charges, which must be notified to

the interested".

In application of the previous precept and taking into account that no

formulated allegations to the initial agreement, it is appropriate to resolve the initiated procedure.

Article 58 of the RGPD, Powers, states:

III

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

corrections listed below:

(…)

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

Instead of the measures mentioned in this section, according to the

circumstances of each particular case;

(…)”

Article 5 of the RGPD establishes the principles that must govern the treatment

of personal data and mentions among them that of “integrity and confidentiality”.

The cited article states 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 appropriate technical or organizational measures ("integrity and

confidentiality”)”.

(…)”

The facts denounced materialize in the abandonment of documentation in

the public road in which personal data corresponding to the claimed person appears,

violating the regulations on data protection.

IV

The security of personal data is regulated in articles 32, 33 and

34 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".

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 abandoned, 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”.

v

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 its systems allowing access to personal data

contained in documents that were abandoned by the claimed party with possible

violation of security measures.

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 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
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/07635/2020 the AEPD transfer to the claimed on

09/28/2020 the written claim presented 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 Foral Police of Navarra, since it is

responsible for making decisions aimed at effectively implementing the

appropriate technical and organizational measures to ensure a level of security

appropriate to the risk to ensure the confidentiality of the data, restoring its

availability and prevent access to them in the event of a physical or technical incident.

However, the documentation provided shows that the entity has not only

breached this obligation, but also the adoption of measures to the

respect, despite having notified him of the claim filed.

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).

In order to establish the administrative fine to be imposed,

observe the provisions contained in articles 83.1 and 83.2 of the RGPD, which

point out:

SAW

"1. Each control authority will guarantee that the imposition of fines

administrative actions under this article for violations of this

Regulation indicated in sections 4, 5 and 6 are in each individual case

effective, proportionate and dissuasive.

2. Administrative fines will be imposed, depending on the circumstances

of each individual case, in addition to or as a substitute for the measures contemplated

in article 58, paragraph 2, letters a) to h) and j). When deciding to impose a fine

administration and its amount in each individual case will be duly taken into account:

a) the nature, seriousness and duration of the offence, taking into account the

nature, scope or purpose of the processing operation in question

as well as the number of stakeholders affected and the level of damage and

damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;

d) the degree of responsibility of the person in charge or of the person in charge of the

treatment, taking into account the technical or organizational measures that have

applied under articles 25 and 32;

e) any previous infraction committed by the person in charge or the person in charge of the

treatment;

f) the degree of cooperation with the supervisory authority in order to put

remedying the breach and mitigating the possible adverse effects of the breach;

g) the categories of personal data affected by the infringement;

h) the way in which the supervisory authority became aware of the infringement, in

particular if the person in charge or the person in charge notified the infringement and, in such case,

what extent;

i) when the measures indicated in article 58, paragraph 2, have been

previously ordered against the person in charge or the person in charge in question

in relation to the same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or mechanisms

certificates approved in accordance with article 42, and

k) any other aggravating or mitigating factor applicable to the circumstances of the

case, such as financial benefits realized or losses avoided, direct

or indirectly, through infringement.

In relation to letter k) of article 83.2 of the RGPD, the LOPDGDD, in its

Article 76, “Sanctions and corrective measures”, establishes that:

"two. In accordance with the provisions of article 83.2.k) of the Regulation (EU)

2016/679 may also be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the performance of treatments

of personal data.

c) The profits obtained as a result of committing the offence.

d) The possibility that the conduct of the affected party could have induced the

commission of the offence.

e) The existence of a merger by absorption process after the commission

of the infringement, which cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

g) Have, when it is not mandatory, a delegate for the protection of

h) The submission by the person in charge or person in charge, with

voluntary, to alternative conflict resolution mechanisms, in those

assumptions in which there are controversies between those and any

interested."

data.

- In accordance with the precepts transcribed, in order to establish the amount

of the sanction of a fine to be imposed in the present case for the infraction typified in the

article 83.4.a) of the RGPD for which the claimed party is responsible, they are estimated

concurrent the following factors:

The merely local scope of the treatment carried out by the claimed party.

The nature and seriousness of the offending conduct as the documentation

abandoned affects the personal data of many people.

The respondent entity does not record that it has adopted measures to prevent the

produce similar incidents; has not responded to the request

information of the Agency which affects the lack of cooperation with the

control authority in order to remedy the infringement and mitigate the

possible side effects of it.

Although there is no evidence that the defendant had acted

intentionally, the conduct observed is deeply negligent.

The link between the activity of the offender and the performance of treatment of

Personal data.

The respondent is a small business.

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 KUKIMBIA S.L., with NIF B99352023, for an infringement of the

Article 32.1 of the RGPD, typified in article 83.4.a) of the RGPD and considered to

prescription effects as a serious infringement, a fine of €3,000 (three thousand euros).

SECOND: NOTIFY this resolution to KUKIMBIA S.L. with NIF

B99352023.

THIRD: Warn the sanctioned party that he must make the imposed sanction effective once

Once this resolution is enforceable, in accordance with the provisions of the

art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (hereinafter LPACAP), within the payment term

voluntary established in art. 68 of the General Collection Regulations, approved

by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,

of December 17, through its entry, indicating the NIF of the sanctioned and the number

of procedure that appears in the heading of this document, in the account

restricted number ES00 0000 0000 0000 0000 0000, opened on behalf of the Agency

Spanish Department of Data Protection in the banking entity CAIXABANK, S.A.. In case

Otherwise, it will be collected in the executive period.

Received the notification and once executed, if the date of execution is

is between the 1st and 15th of each month, both inclusive, the term to carry out the

voluntary payment will be until the 20th day of the following month or immediately after, and if

is between the 16th and last day of each month, both inclusive, the term of the

payment will be until the 5th of the second following month or immediately after.

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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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