 File No.: PS/00101/2022

RESOLUTION OF SANCTIONING 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 claiming party) dated May 17, 2021

filed a claim with the Spanish Data Protection Agency.

The claim is directed against RESTEXPERIENCE, S.L. with NIF B88260609 (in

below, the claimed party).

The reasons on which the claim is based are the following:

The claimant states that on April 7, 2021, she requested the Director of Operations and

EXPANSION OF THE RESTEXPERIENCE GROUP your withholding certificate.

On May 5, 2021, the COO emailed the

claimant and 11 other recipients a PDF file containing the certificate of

withholdings of 36 company workers.

Along with the claim, provide the email sent on June 5, 2021 along with the file

annexed.

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

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

forward LOPDGDD), on June 14, 2021, said claim was transferred to the

claimed party, to proceed with its analysis and inform this Agency in the

period of one month, of the actions carried out to adapt to the requirements

provided for in the data protection regulations.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

Public (hereinafter, LPACAP) by electronic notification, was not collected by

the person in charge, within the period of availability, understood as rejected

in accordance with the provisions of art. 43.2 of the LPACAP dated June 25, 2021

as stated in the certificate that is in the file.

THIRD: On September 7, 2021, in accordance with article 65 of

the LOPDGDD, the claim presented by the complaining party was admitted for processing.

FOURTH: The General Subdirectorate of Data Inspection proceeded to carry out

of previous investigative actions to clarify the facts in

matter, by virtue of the functions assigned to the control authorities in the

article 57.1 and the powers granted in article 58.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter GDPR), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the

LOPDGDD, having knowledge of the following extremes:

(…).

Information and documentation has been requested from the responsible entity, and from the

The response received shows the following:

Regarding the chronology of the events and actions taken in order to minimize

the adverse effects and measures adopted for their final resolution

(…).

(…).

Regarding the causes that made the gap possible

(…).

Regarding the affected data

(…).

Regarding the treatment manager contract

(…).

Regarding the security measures implemented:

(…).

(…):

(…).

(…):

(…)

(…)

(…)

(…):

-

-

(…).

(…).

-

(…)

(…)

Regarding notification after 72 hours

(…)

Information on the recurrence of these events and number of similar events

events in time

(…)

FIFTH: On May 31, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate disciplinary proceedings against the claimed party,

in accordance with the provisions of articles 63 and 64 of Law 39/2015, of October 1,

of the Common Administrative Procedure of Public Administrations (in

hereinafter, LPACAP), for the alleged infringement of article 5.1.f) of the GDPR and article

32 of the GDPR, typified in Article 83.5 of the GDPR.

SIXTH: On June 10, 2022, the claimed party submitted a written

allegations in which, in summary, it stated that "this party recognizes the

responsibility that is being imputed to him and for this reason he requests that the

timely reduction of the penalty. Likewise, it informs the AGEPD that

the intention of the company would be to pay the voluntary payment of the

sanction imposed, however, the negative economic situation in which

finds it does not allow it".

SEVENTH: On July 6, 2022, the procedure instructor agreed to consider

reproduced for evidentiary purposes the claim filed by A.A.A. and his

documentation, the documents obtained and generated during the admission phase to

processing of the claim, and the report of previous investigation actions that

are part of the procedure.

Likewise, it is considered reproduced for evidentiary purposes, the allegations to the

start of

submitted by

RESTEXPERIENCE, S.L., and the accompanying documentation.

disciplinary procedure

referenced,

EIGHTH: On July 15, 2022, a resolution proposal was formulated,

proposing that the Director of the Spanish Data Protection Agency

sanction RESTEXPERIENCE, S.L., with NIF B88260609, for a violation of the

article 5.1.f) of the GDPR and for a second infringement of article 32 of the GDPR,

typified respectively in articles 83.5 a) and 83.4 a) of the GDPR, with a fine

of 3,000 euros (three thousand euros) and 2,000 euros (two thousand euros) respectively.

Of the actions carried out in this procedure and of the documentation

in the file, the following have been accredited:

PROVEN FACTS

FIRST: The claimed entity has emailed the claimant and

11 more people, the withholding certificate for 36 people, violating the

confidentiality required in the processing of personal data, as well as the principle

of integrity and confidentiality, so that the data is treated in such a way that

adequate security of personal data is ensured.

SECOND: The claimed entity acknowledges the infractions committed and requests the

double reduction for acknowledgment of the infraction and prompt payment, but alleges that it does not

you can proceed to the same.

FUNDAMENTALS OF LAW

Yo

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

control, and as established in articles 47 and 48 of the LOPDGDD, the Director

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

solve this procedure.

II

The principles related to the processing of personal data are regulated in the

Article 5 of the GDPR which establishes that "personal data will be:

"a) treated in a lawful, loyal and transparent manner in relation to the interested party ("lawfulness,

loyalty and transparency»);

b) collected for specific, explicit and legitimate purposes, and will not be processed

subsequently in a manner incompatible with said purposes; according to article 89,

paragraph 1, the further processing of personal data for archiving purposes in

public interest, scientific and historical research purposes or statistical purposes shall not be

considered incompatible with the initial purposes ("purpose limitation");

c) adequate, pertinent and limited to what is necessary in relation to the purposes for which

that are processed ("data minimization");

d) accurate and, if necessary, up-to-date; all measures will be taken

Reasonable reasons for the erasure or rectification without delay of the personal data

are inaccurate with respect to the purposes for which they are processed ("accuracy");

e) maintained in such a way that the identification of the interested parties is allowed during

longer than necessary for the purposes of processing personal data; the

personal data may be retained for longer periods as long as

processed exclusively for archiving purposes in the public interest, research purposes

scientific or historical or statistical purposes, in accordance with article 89, paragraph 1,

without prejudice to the application of appropriate technical and organizational measures that

imposes this Regulation in order to protect the rights and freedoms of the

data subject ("retention period limitation");

f) processed in such a way as to guarantee adequate data security

personal data, including protection against unauthorized or unlawful processing and against

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

or organizational ("integrity and confidentiality").

The controller will be responsible for compliance with the provisions of

paragraph 1 and able to demonstrate it ("proactive responsibility")."

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 in violation of the principles and guarantees

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

II

Security in the processing of personal data is regulated in article 32 of the

GDPR where the following is established:

"1. Taking into account the state of the art, the application costs, and the nature of

nature, scope, context and purposes of processing, as well as probability risks

and variable severity for the rights and freedoms of natural persons, the responsibility

responsible and the person in charge of the treatment will apply appropriate technical and organizational measures.

measures to guarantee a level of security appropriate to the risk, which, where appropriate, will include

yeah, among others:

a) the pseudonymization and encryption of personal data;

b) the ability to ensure confidentiality, integrity, availability and resilience

permanent treatment systems and services;

c) the ability to restore the availability and access to the personal data of

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 assessing the adequacy of the security level, particular account shall be taken of

The risks presented by the data processing, in particular as a consequence

of the destruction, loss or accidental or illegal alteration of personal data transmitted

collected, preserved or processed in another way, or the unauthorized communication or access

two to said data.

3. Adherence to a code of conduct approved under article 40 or to a mecha-

certification document approved in accordance with article 42 may serve as an element to

demonstrate compliance with the requirements established in section 1 of this

article.

4. The controller and the processor shall take measures to ensure that

any person acting under the authority of the controller or processor and having

ga access to personal data can only process such data following instructions

of the controller, unless it is required to do so by Union law or by

the Member States."

Article 73.f) of the LOPDGDD, under the heading "Infringements considered serious

has:

"Based on article 83.4 of Regulation (EU) 2016/679, serious and

Offenses that involve a substantial violation of the law shall prescribe after two years.

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

IV.

In accordance with the available evidence, corroborated with the

allegations made by the claimant on June 10, 2022, indicating that

recognizes the facts that are imputed to him, but that he cannot proceed immediately

payment due to the current economic situation, it is considered that the entity claimed at

send the claimant and 11 other recipients a PDF file by email

which contains the withholding certificate of 36 company workers, has

violated the confidentiality required in the processing of personal data, and with

This contravenes article 5.1 f) of the GDPR, which governs the principle of integrity and

confidentiality, so that the data is treated in such a way as to guarantee a

adequate security of personal data, including protection against

unauthorized or illegal treatment and against its loss, destruction or accidental damage,

through the application of appropriate technical or organizational measures.

It should be noted that the requested entity has stated that this incident does not

was identified as a security breach until the transfer of this information was received

claim and, for this reason, the data protection delegate was not informed nor

its scope was analyzed to assess the notification to the interested parties or to the AEPD.

Likewise, the requested entity considers that the security measures implemented

are audited every two years in terms of data protection, where

specifically review the procedures for sending documentation that

contain personal data.

The requested entity considers that there is no risk to the rights and freedoms

of those affected, and that there is no record of the use of the data by third parties apart from the

presentation of this claim before the AEPD.

Despite what has been indicated, this Agency considers that the existence of a single case is

sufficient to denote that the security measures of the claimed entity were not

appropriate at the time of the incident that is the subject of the claim and must

be improved because it is verified that they have not been sufficient to avoid the

reported facts.

Thus, this Agency considers that the claimed entity has infringed the

Articles 5.1 f) and 32 of the GDPR, by violating the principle of integrity and confidentiality, as well

such as not adopting the necessary security measures to guarantee the protection of

the personal data of its customers.

V

Article 58.2 of the GDPR provides the following: "Each control authority shall have

of all of the following corrective powers listed below:

d) order the person in charge or person 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 in accordance with article 83, in addition to or instead of the

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

particular;

SAW

In order to determine the administrative fines to be imposed, the

provisions of articles 83.1 and 83.2 of the GDPR, precepts that state:

"Each control authority will guarantee that the imposition of administrative fines

under this Article for infringements of this Regulation

indicated in sections 4, 9 and 6 are effective in each individual case,

proportionate and dissuasive."

"Administrative fines will be imposed, depending on the circumstances of each

individual case, in addition to or in lieu of 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 shall be duly taken into account:

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

nature, scope or purpose of the processing operation in question, as well as the number

number of interested parties affected and the level of damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the person in charge or in charge of the treatment to

settle 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, habi-

gives an account of the technical or organizational measures that have been applied by virtue of the

articles 25 and 32;

e) any previous infringement committed by the controller or processor;

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

infringement and mitigate the possible adverse effects of the infringement;

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

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

8/10

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

determine whether the controller or processor notified the infringement and, if so, to what extent

gives;

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

previously against the person in charge or the person in charge in relation to the

same matter, compliance with said measures;

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

fications approved in accordance with article 42, and

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

as the financial benefits obtained or the losses avoided, directly or indirectly.

mind, through infraction."

Regarding section k) of article 83.2 of the GDPR, the LOPDGDD, article 76,

"Sanctions and corrective measures", provides:

"2. In accordance with the provisions of article 83.2.k) of 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 data processing.

personal information.

c) The benefits obtained as a consequence of the commission of the infraction.

d) The possibility that the conduct of the affected party could have led to the commission

of the offence.

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

violation, which cannot be attributed to the absorbing entity.

f) The affectation of the rights of minors.

g) Have, when it is not mandatory, a data protection delegate.

h) Submission by the person responsible or in charge, on a voluntary basis, to

alternative conflict resolution mechanisms, in those cases in which

there are controversies between those and any interested party."

VII

Violation of article 5.1 f) of the GDPR may be punished with a fine of 20,000

€000 maximum or, in the case of a company, an amount equivalent to 4%

maximum of the overall annual total turnover of the financial year

above, opting for the one with the highest amount, in accordance with article 83.5 of the

GDPR.

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the

following criteria established in article 83.2 of the GDPR, considering as

aggravating circumstance according to article 76.2 b) LOPDGDD, the relationship of the person responsible with the

processing of personal data, and the number of affected parties, having sent data

personal of 36 people.

VIII

The violation of article 32 of the GDPR can be sanctioned with a fine of 10,000,000

€ maximum or, in the case of a company, an amount equivalent to 2%

maximum of the overall annual total turnover of the financial year

above, opting for the one with the highest amount, in accordance with article 83.4 of the

GDPR.

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the

following criteria established in article 83.2 of the GDPR, considering as

aggravating circumstance according to article 76.2 b) LOPDGDD, the relationship of the person responsible with the

processing of personal data and the number of affected parties, having sent data

personal of 36 people.

Therefore, in accordance with the applicable legislation and assessed the criteria of

graduation of sanctions whose existence has been accredited,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE RESTEXPERIENCE, S.L., with NIF B88260609, for a

violation of article 5.1.f) of the GDPR and for a second violation of article 32 of the

GDPR, typified respectively in articles 83.5 a) and 83.4 a) of the GDPR, a

fine of 3,000 euros (three thousand euros) and another of 2,000 euros (two thousand euros)

respectively.

SECOND: NOTIFY this resolution to RESTEXPERIENCE, S.L.

THIRD: Warn the penalized person that they must make the imposed sanction effective

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

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

Common of Public Administrations (hereinafter LPACAP), within the payment period

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, by means of its income, 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, open in the name of the Agency

Spanish Data Protection Agency at the bank CAIXABANK, S.A.. In the event

Otherwise, it will proceed to its collection in the executive period.

Once the notification has been received and once executed, if the execution date is

between the 1st and 15th of each month, both inclusive, the term to make the payment

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

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

It will be until the 5th of the second following or immediately following business month.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process 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 reversal before the

Director of the Spanish Agency for Data Protection within a period of one month from

count 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 for in article 46.1 of the

referred Law.

Finally, it is noted 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 through

writing addressed to the Spanish Data Protection Agency, presenting it through

of the Electronic Registry of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registries 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 proceedings within a period of two months from the day following the

Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

938-120722

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es