 File No.: EXP202204631

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: Ms. A.A.A., in the name and representation of D. B.B.B., D. C.C.C., D. D.D.D.

and D.E.E.E. (hereinafter, the claimant), on March 16, 2022,

filed a claim with the Spanish Data Protection Agency. The

claim is directed against the ARAGONES UNION OF WORKERS OF THE

TRANSPORTATION, with NIF G99300667 (hereinafter, the claimed party).

The claimants are members of the strike committee in the context of a conflict

collective agreement between the company Avanza Zaragoza SAU and its workers. The

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

They state that, due to a collective conflict that arose between workers and

company, on February 11, 2022, the defendant published on social networks

(Facebook, Twitter) and on its website, a document in which the data appeared

personal information (name, surname and ID) of the members of the strike committee.

The aforementioned publication with the personal data of those affected was, at

Apparently, at least half an hour visible within the reach of anyone. Subsequently

the publication was rectified, as a consequence of the complaints expressed.

Along with the claim, a copy of the publication is provided, as well as a printout of

screen of a WhatsApp conversation in which it is revealed between the

workers the aforementioned publication, as well as the fact that it was available

publicly for half an hour.

The publication has been attached as it is currently available, stating

blurred the personal data of those affected (***URL.1)

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

December, Protection of Personal Data and Guarantee of Digital Rights

(hereinafter LOPDGDD), said claim was transferred to the claimed party,

to proceed with its analysis and inform this Agency within a month,

of the actions carried out to adapt to the requirements established 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 May 2, 2022,

as stated in the certificate that is in the file.

Although the notification was validly made by electronic means, assuming that

carried out the procedure in accordance with the provisions of article 41.5 of the LPACAP, under

informative, a copy was sent by postal mail that was returned by the Service of

Correos, dated May 16, 2022, due to absence during delivery hours. in bliss

notification, they were reminded of their obligation to interact electronically with the

Administration, and was informed of the means of access to said notifications,

reiterating that, henceforth, you will be notified exclusively by means

electronics.

On May 27, 2022, the transfer was reiterated by certified postal mail, which

it was again returned for "absent" on June 7, 2022.

No response has been received to this letter of transfer.

THIRD: On June 16, 2022, in accordance with article 65 of the

LOPDGDD, the admission for processing of the claim presented by the

complaining party.

FOURTH: On August 10, 2022, the Director of the Spanish Agency for

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

for the alleged violation of article 5.1.f) of the GDPR and article 32 of the GDPR,

typified in articles 83.5 and 83.4 of the GDPR, respectively

The initiation agreement was mailed and returned by the Postal Service by

"unknown", proceeding to its publication in the Official State Gazette, on date

August 31, 2022, in accordance with the provisions of article 44 of the Law

39/2015, of October 1, of the Common Administrative Procedure of the Administrations

Public tions.

FIFTH: Notified of the aforementioned start-up agreement in accordance with the rules established in

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

Public Administrations (hereinafter, LPACAP) and after the period granted

for the formulation of allegations, it has been verified that no allegation has been received

any by the claimed party.

Article 64.2.f) of the LPACAP -provision of which the claimed party was informed

in the agreement to open the procedure - establishes that if no

arguments within the established term on the content of the initiation agreement, when

it contains a precise pronouncement about the imputed responsibility,

may be considered a resolution proposal. In the present case, the agreement of

beginning of the disciplinary file determined the facts in which the

imputation, the infringement of the GDPR attributed to the defendant and the sanction that could impose. Therefore, taking into consideration that the claimed party has not made allegations to the agreement to start the file and in attention to what established in article 64.2.f) of the LPACAP, the aforementioned initiation agreement is considered in the present case resolution proposal.

In view of all the proceedings, by the Spanish Agency for Data Protection In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: It is on record that on March 16, 2022, the claimant filed claim before the Spanish Data Protection Agency, since the party claimed revealed information and personal data to third parties, without legal basis legitimizing for this, by publishing on social networks, a document in which the personal data (name, surname and ID) of the committee members appeared of strike.

SECOND: There is a copy of the publication, as well as a screen print of a WhatsApp conversation in which it is revealed among the workers the cited publication.

FUNDAMENTALS OF LAW

Yo

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter GDPR), grants each

control authority and as established in articles 47, 48.1, 64.2 and 68.1 of the

Organic Law 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 Agency for

Data Protection.

Likewise, article 63.2 of the LOPDGDD determines that: "The procedures

processed by the Spanish Data Protection Agency will be governed by the provisions

in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations dictated in its development and, insofar as they do not contradict them, with character

subsidiary, by the general rules on administrative procedures."

II

previous questions

In the present case, in accordance with the provisions of article 4.1 of the GDPR, there is

the processing of personal data, since the UNION

ARAGONES OF TRANSPORT WORKERS, in the exercise of their activity

trade union and advice, performs personal data processing in its relationship with the

affiliates.

It carries out this activity in its capacity as data controller, since it is

who determines the purposes and means of such activity, by virtue of article 4.7 of the GDPR:

"responsible for the treatment" or "responsible": the natural or legal person, authority

public authority, service or other body that, alone or jointly with others, determines the purposes and

means of treatment; if the law of the Union or of the Member States determines

determines the purposes and means of the treatment, the person in charge of the treatment or the criteria

Specific reasons for their appointment may be established by the Law of the Union or of the Member states.

Article 4 section 12 of the RGPD defines, in a broad way, the "violations of security" security of personal data" (hereinafter security breach) as "all those security violations that cause the destruction, loss or alteration Accidental or illegal transfer of personal data transmitted, stored or processed in otherwise, or unauthorized communication or access to such data."

In the present case, there is a personal data security breach in the circumstances indicated above, categorized as a breach of confidentiality, whenever the claimed party has disclosed information and data of a personal nature to third parties, without legitimizing legal basis for it, when publishing on social networks, a document in which the personal data (name, surname and ID) of the members of the strike committee, with the multiplying effects that the use of the social media may have for your visibility.

According to GT29, a "Breach of confidentiality" occurs when there is an unauthorized or accidental disclosure of personal data, or access to it themselves.

It should be noted that the identification of a security breach does not imply the impossibility sanction directly by this Agency, since it is necessary to analyze the diligence of managers and managers and security measures applied.

Within the principles of treatment provided for in article 5 of the GDPR, the integrity and confidentiality of personal data is guaranteed in section 1.f) of article 5 of the GDPR. For its part, the security of personal data comes regulated in article 32 of the GDPR.

II

Article 5.1.f) of the GDPR

Article 5.1.f) of the GDPR establishes the following:

"Article 5 Principles relating to treatment:

1. Personal data will be:

(…)

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 procedures (“integrity and confidentiality”).”

In relation to this principle, Recital 39 of the aforementioned GDPR states that:

“[…]Personal data must be processed in a way that guarantees security and

appropriate confidentiality of personal data, including to prevent access

or unauthorized use of said data and of the equipment used in the treatment”.

The documentation in the file offers clear indications that the

claimed violated article 5.1 f) of the GDPR, principles relating to treatment.

The post exposed by the claimed party in the social networks supposes a treatment

automated system that, using the infrastructure of said networks, discloses some

facts and data that allow the claimants to be identified through the

exposed information, and said infrastructure is also a medium in which

They can multiply their effects by sharing the news with other users.

Consequently, it is considered that the accredited facts are constitutive of

infringement, attributable to the claimed party, due to violation of article 5.1.f) of the

GDPR.

Classification of the infringement of article 5.1.f) of the GDPR

IV.

The aforementioned infringement of article 5.1.f) of the GDPR supposes the commission of the infringements

typified in article 83.5 of the GDPR that under the heading "General conditions

for the imposition of administrative fines" provides:

Violations of the following provisions will be sanctioned, in accordance with the

paragraph 2, with administrative fines of maximum EUR 20,000,000 or,

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

total annual global business volume of the previous financial year, opting for

the highest amount:

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

to)

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

In this regard, the LOPDGDD, in its article 71 "Infractions" 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 72 "Infractions considered very

serious" of the LOPDGDD indicates:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679,

are considered very serious and will prescribe after three years the infractions that

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. (…)”

V

GDPR Article 32

Article 32 of the GDPR, security of treatment, establishes the following:

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

nature, scope, context and purposes of processing, 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 and

appropriate organizational measures to guarantee a level of security appropriate to the risk,

which may include, among others:

a) the 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 assessment of effectiveness

technical and organizational measures to guarantee the safety of the

treatment.

2. When evaluating the adequacy of the security level, particular consideration will be given to

take into account the risks presented by data processing, in particular as

consequence of the destruction, loss or accidental or illegal alteration of data

personal information transmitted, preserved or processed in another way, or the communication or

unauthorized access to such data.

3. Adherence to an approved code of conduct pursuant to 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 controller and the processor shall take measures to ensure that

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

have access to personal data can only process such data by following

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.

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

claimed has violated article 32 of the GDPR, when a security incident occurred

by publishing a document in which personal data appeared (name, last name,

ID) of the members of the strike committee, without having the technical measures

appropriate cas and organizational

It should be noted that the GDPR in the aforementioned precept does not establish a list of the

security measures that are applicable according to the data that is the object

of treatment, but it 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 processing, probability risks

and seriousness for the rights and freedoms of the persons concerned.

In addition, security measures must be adequate and proportionate to the

detected risk, noting that the determination of the technical measures and

organizational procedures must be carried out taking into account: pseudonymization and encryption, the

ability to ensure 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 security level,

particular account of the risks presented by data processing, such as

consequence of the destruction, loss or accidental or illegal alteration of data

personal information transmitted, preserved or processed in another way, or the communication or

unauthorized access to said data and that could cause damages

physical, material or immaterial.

In this sense, recital 83 of the GDPR states that:

"(83) In order to maintain security and prevent processing from infringing what

provided in this Regulation, the person in charge or in charge must evaluate

the risks inherent to the treatment and apply measures to mitigate them, such as the

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 nature of the personal data to be

protect yourself. When assessing risk in relation to data security, considerations should be

take into account the risks arising from the processing of personal data,

such as the destruction, loss or accidental or unlawful alteration of personal data

transmitted, stored or processed in another way, or communication or access not
authorized to said data, susceptible in particular to cause damages
physical, material or immaterial.
The responsibility of the defendant is determined by the lack of measures of
security, 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, from the documentation provided it appears that the
entity has not only breached this obligation, but also the
adoption of measures in this regard, despite having notified him of the claim
presented.
Therefore, the accredited facts constitute an infraction, attributable to the
claimed party, for violation of article 32 GDPR.
Classification of the infringement of article 32 of the GDPR
SAW
The aforementioned infringement of article 32 of the GDPR supposes the commission of the infringements
typified in article 83.4 of the GDPR that under the heading "General conditions
for the imposition of administrative fines" provides:
Violations of the following provisions will be sanctioned, in accordance with the
paragraph 2, with administrative fines of maximum EUR 10,000,000 or,
in the case of a company, an amount equivalent to a maximum of 2% of the

total annual global business volume of the previous financial year, opting for

the highest amount:

to)

the obligations of the controller and the person in charge under articles 8,

11, 25 to 39, 42 and 43; (…)”

In this regard, the LOPDGDD, in its article 71 "Infractions" 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 "Infractions considered serious"

of the LOPDGDD indicates:

"Based on what is established in 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:

f) The lack of adoption of those technical and organizational measures that

are appropriate to ensure a level of security appropriate to the

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

Regulation (EU) 2016/679.”

VII

Sanction

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

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

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

administrative proceedings under this article for violations of this

Regulations 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 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;

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

given 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,

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."

For its part, article 76 "Sanctions and corrective measures" of the LOPDGDD

has:

"1. The sanctions provided for in sections 4, 5 and 6 of article 83 of the Regulation

(UE) 2016/679 will be applied taking into account the graduation criteria

established in section 2 of said article.

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) Linking the activity of the offender with the performance of processing

of personal data.

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 process by absorption after the commission

of the infringement, 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) The submission by the person in charge or in charge, with character

voluntary, alternative conflict resolution mechanisms, in those

cases in which there are controversies between those and any

interested."

data.

Considering the exposed factors, the valuation that reaches the amount of the fine

is €2,000 for violation of article 5.1 f) of the GDPR, regarding the violation of the

principle of confidentiality and €1,000 for violation of article 32 of the aforementioned

GDPR, regarding the security of personal data processing.

VIII

Responsibility

Establishes Law 40/2015, of October 1, on the Legal Regime of the Public Sector, in

Chapter III relating to the "Principles of the Power to sanction", in article 28

under the heading "Responsibility", the following:

"1. They may only be penalized for acts constituting an administrative offense

physical and legal persons, as well as, when a Law recognizes their capacity to

act, the affected groups, the unions and entities without legal personality and the

independent or autonomous patrimonies, which are responsible for them

title of fraud or fault."

Lack of diligence in implementing appropriate security measures

with the consequence of the breach of the principle of confidentiality constitutes the

element of guilt.

IX

Measures

Likewise, it is appropriate to impose the corrective measure described in article 58.2.d) of the GDPR and order the claimed party to, within a month, establish the adequate security measures so that the treatments are adapted to the requirements contemplated in articles 5.1 f) and 32 of the GDPR, preventing the similar situations occur in the future.

The text of the resolution establishes which have been the infractions committed and the facts that have given rise to the violation of the regulations for the protection of data, from which it is clearly inferred what are the measures to adopt, without prejudice that the type of procedures, mechanisms or concrete instruments for implement them corresponds to the sanctioned party, since it is responsible for the treatment who fully knows its organization and has to decide, based on the proactive responsibility and risk approach, how to comply with the GDPR and the LOPDGDD.

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 the ARAGONESE UNION OF WORKERS OF THE TRANSPORTATION, with NIF G99300667,

- for a violation of article 5.1.f) of the GDPR, classified in accordance with the provisions of Article 83.5 of the GDPR, classified as very serious for the purposes of prescription in the article 72.1 a) of the LOPDGDD, a fine of €2,000.

- for a violation of article 32 of the GDPR, classified in accordance with the provisions of article article 83.4 of the GDPR, classified as serious for the purposes of prescription in article 73 f) of the LOPDGDD, a fine of €1,000.

SECOND: REQUEST the ARAGONESE UNION OF WORKERS OF THE

TRANSPORTATION, with NIF G99300667 that implements, within a month, the measures

corrections necessary to adapt its performance to the regulations for the protection of

personal data, which prevent similar events from being repeated in the future, as well as

to inform this Agency, within the same term, about the measures adopted.

THIRD: NOTIFY this resolution to the ARAGONESE UNION OF

TRANSPORT WORKERS.

FOURTH: Warn the sanctioned party that he must enforce the sanction imposed

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 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, 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

IBAN: ES00-0000-0000-0000-0000-0000 (BIC/SWIFT Code:

restricted no.

00000000000), opened in the name of the Spanish Data Protection Agency in the

banking entity CAIXABANK, S.A. Otherwise, it will be collected

in 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

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

938-181022

12/12

Director of the Spanish Data Protection Agency

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es