

□ File No.: PS/00332/2021

## RESOLUTION OF PUNISHMENT PROCEDURE

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

### BACKGROUND

FIRST: On October 23, 2019, D. A.A.A. and Mrs. B.B.B., hereinafter the  
claimants, filed a claim with the Spanish Protection Agency  
of Data, against the MUNICIPAL TRANSPORT COMPANY OF \*\*\*LOCALITY.1  
S.A.U., with CIF A46318416 (hereinafter, the claimed party), in relation to an alleged  
violation of article 32 of Regulation (EU) 2016/679, of April 27, 2016 (in  
forward, GDPR).

In their statement of claim, the claimants (members of the Council of  
Administration of the Municipal Transport Company of \*\*\*LOCATION.1),  
stated that on September 27, 2019, in an extraordinary session,  
they were informed of an alleged fraud of more than 4 million euros, for an alleged  
identity theft of the company's management personnel, with payment orders,  
which was a serious security breach.

Not knowing if this Agency had been informed, as  
provided in the RGPD, on November 15, 2019, the claimants sent  
written before the refusal of the Municipal Transport Company of \*\*\*LOCATION.1  
to inform this Agency and the National Cryptologic Center about the breach of  
security that occurred in September 2019, requesting that the pertinent  
sanction file.

SECOND: On November 29, 2019, the claimants submit a new written  
in which they expand the object of the complaint when it is verified in the audits carried out to

the Municipal Transport Company of \*\*\* LOCALITY.1, the breach of the RGD, requesting that it be investigated. Among the documentation provided find the Cybersecurity Action Plan, the Security Plan document of the claimed, documents of the audit and consultancy service for the implementation of the RGD prepared by an auditing firm for the claimed and the expert opinion prepared by Telefónica that was already provided by the defendant.

THIRD: 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 respondent, so that proceed to its analysis and inform this Agency within a month of the actions carried out to adapt to the requirements set forth in the regulations of Data Protection.

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

2/8

There is evidence in this Agency of the reply to the transfer of the claim, by means of writings dated February 21 and 24, 2020.

FOURTH: On June 1, 2020, after analyzing the documentation that was in the file, a resolution was issued by the Director of the AEPD, agreeing to file of the claim. The resolution was notified to the claimants, on June 3 2020, according to confirmation of receipt that appears in the file.

FIFTH: On July 2, 2020, the claimants filed an appeal optional replacement through the Electronic Registry of the AEPD, against the resolution relapsed in file E/11294/2019, in which they show their

disagreement with the contested resolution, stating that the resolution is not corresponds to the facts denounced and that have been resolved at the same time three different claims. They also do not know if the security breach was communicated to this Agency and that it has not been resolved on the lack of adaptation to the GDPR. They also note that the entire file was not attached to the transfer of the claim to the claimed one missing the documentation sent on 15 and November 29, 2019 and request that the resolution be declared null and void and agree to investigate the reported facts.

SIXTH: On February 12, 2021, the claimants submit a new written

Extension of the resource to which two documents are attached:

☐ Report on activities for the 2019 financial year of the agency for the prevention and fight against fraud and corruption of the Community \*\*\*LOCATION.1 of 30 of March 2020.

☐

Safety audit report of the Municipal Transport Company of

\*\*\*LOCALIDAD.1 SAU, for fiscal year 2020, in which the claimant states

that the non-compliance by the respondent with what is

established by the personal data protection regulations and their

adaptation to the RGD.

SEVENTH: On February 26, 2021, the Director of the Spanish Agency for

Data Protection resolves to estimate the reversal appeal filed and agrees to the

Admission to processing of the claim filed against MUNICIPAL COMPANY OF

TRANSPORTATION OF \*\*\*LOCALITY.1 S.A.U.

EIGHTH: In view of the notified facts and the documents provided, the

Subdirector General for Data Inspection proceeded to carry out actions

preliminary investigations to clarify the facts described in the

previous sections, by virtue of the powers of investigation granted to the control authorities in article 57.1 of Regulation (EU) 2016/679 (Regulation General Data Protection, hereinafter RGPD), and in accordance with the established in Title VII, Chapter I, Second Section, of Organic Law 3/2018, of December 5, Protection of Personal Data and Guarantee of Rights Digital (hereinafter LOPDGDD), having knowledge of the following ends:

Regarding the security breach of personal data

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

3/8

In the response brief of the accused within the framework of the actions of reference E/11294/2019, state the following:

(...).

Regarding the causes that made the gap possible:

(...).

Affected data:

(...).

Communication to those affected:

(...).

Regarding notification after 72 hours.

(...).

Regarding the security measures implemented

(...).

The EMT representative provides a copy of the document called "Meeting of cybersecurity compliance degree monitoring" prepared by XX on \*\*\*DATE.1.

The document shows that the following tasks have been completed:

(...).

The document states that the following work has been carried out:

(...).

-

The EMT representative provides a copy of the document "Meeting of

-

Monitoring degree of compliance in Data Protection and Cybersecurity. Service advice and consultancy for the implementation of the General Protection Regulation (RGPD) and National Security Scheme (ENS) for EMT

\*\*\*LOCATION.1 Exp. – \*\*\*EXP.1. \*\*\*DATE.2", in which the situation is specified current adaptation to the RGPD of the EMT:

(...).

-

They provide a copy of the document "\*\*\*\*DOCUMENTO.1, \*\*\*LOCALIDAD.1, SAU",

-

prepared by the Audit Office of the Community \*\*\*LOCALIDAD.1, in which collects the report of the cybersecurity audit of the Municipal Company of Transportes de \*\*\*LOCALIDAD.1, S.A.U., focused on the areas of income from passenger transport, accounting and treasury, referring to the status of controls during 2020, whose conclusions are:

(...).

-

-

They provide impact assessment of the treatments “Title management personal”, “Management of non-personal titles”, “Staff recruitment” and “video surveillance”, undated, in which the threats and security controls are defined. security based on the requirements of the RGPD and the ISO 27002 standard. They provide a copy of the document “Procedure for managing privacy incidents and security breaches of personal data”, whose objective is to define a process of [www.aepd.es](http://www.aepd.es)

C/ Jorge Juan, 6

28001 – Madrid

[sedeagpd.gob.es](http://sedeagpd.gob.es)

4/8

management of privacy incidents and security breaches of personal data, of in accordance with the RGPD, and specifically in its articles 33 and 34. (...).

NINTH: On September 1, 2021, the Director of the Spanish Agency for Data Protection agreed to initiate a sanctioning procedure against the investigated entity, for the alleged infringement of article 32 of the RGPD, typified in article 83.4 of the GDPR.

Notified of the initiation agreement, the investigated entity submitted a written statement of allegations in which, in summary, it stated the following:

1. That he is completely defenseless regarding the facts and reasons that have substantiated the agreement to initiate the sanctioning procedure whenever who were not aware of the challenge to file the proceedings, the appeal for reversal filed, as well as the brief dated February 12, 2021, nor of the Resolution dated February 26, 2021.

2. The facts do not occur as a result of human error but by the

lack of diligence and non-compliance with the existing measures in the EMT by

of which she was Director of Administration of EMT.

3. There has been no direct access to the information or to the information systems

EMT, therefore not being a security breach.

4. The data communicated were exclusively the D.N.I. of two people, who

include their signatures.

5. There was a quick reaction by EMT and the situation was put in

knowledge of the interested parties immediately at the moment in which the

knew the facts, without there having been any economic damage to the

interested.

6. Although the data communicated make the interested parties identifiable, they were

used exclusively in their capacity as senior EMT management personnel when

purpose of eluding the security policies regarding patrimonial dispositions.

7. EMT, in its capacity as data controller, has implemented the

technical and organizational measures that guarantee compliance with regulations

in terms of data protection, having already been contributed to this

process. As is evident, even these measures were reinforced as a result of the

knowledge of the facts

8. If there has been any sanctionable conduct, said sanction, in accordance

with article 77.1 c) of LO 3/2018 of December 5 on Data Protection and

Guarantee of Digital Rights, in relation to the second section of the

The same article should consist of a warning.

9. Documentation is provided regarding the Record of Processing Activities and

Risk Analysis on them.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/8

TENTH: On October 11, 2021, a resolution proposal was formulated,

proposing:

<< That the Director of the Spanish Agency for Data Protection directs a

warning to the MUNICIPAL TRANSPORT COMPANY OF \*\*\*LOCALITY.1

S.A.U., with NIF A46318416, for an infringement of article 32 of the RGPD, typified in

article 83.4 of the RGPD.>>

ELEVEN: On October 27, 2021, the investigated entity submits a written

of allegations to the Resolution Proposal, in which, in summary, it states that

has violated their right to defense, since they were not aware of the

optional appeal for reconsideration, or the extension of the aforementioned appeal or its

resolution, shows its disagreement with the alleged violation of article 32 of the

RGPD, states that the events did not occur as a result of an error

but by the lack of diligence and non-compliance with the existing measures by

part of which was Director of administration, that there was a quick reaction and the

The situation was brought to the attention of the interested parties immediately, which

there was sufficient fault in the facts provided for in this proceeding and requests

the annulment of the procedure.

In view of everything that has been done, by the Spanish Data Protection Agency

In this proceeding, the following are considered proven facts:

FACTS

FIRST: On October 23, 2019, the claimants filed a

claim before the Spanish Agency for Data Protection, against the COMPANY

MUNICIPAL DE TRANSPORTES DE \*\*\*LOCALIDAD.1 S.A.U., with CIF A46318416,



in relation to an alleged violation of Article 32 of the Regulation (EU)

2016/679, of April 27, 2016 (hereinafter, RGPD).

SECOND: In view of the notified facts and the documents provided, the Subdirector General for Data Inspection proceeded to carry out actions prior investigation to clarify the facts, by virtue of the investigative powers granted to the control authorities in article 57.1 of the Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter RGPD), and in accordance with the provisions of Title VII, Chapter I, Section second, of Organic Law 3/2018, of December 5, on Data Protection Personal and Guarantee of Digital Rights (hereinafter LOPDGDD), having knowledge of the previous deficiencies in the security measures, techniques and organizational, existing before the phishing attack. (facts investigated by the Investigating Court number 18 of Valencia, in Preliminary Proceedings 1764/2019).

THIRD: At present, the investigated entity has provided documentation that certifies the progressive implementation of security, technical and organizational, necessary to avoid similar events in the future. The documentation provided is incorporated into the file.

FOUNDATIONS OF LAW

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

6/8

FIRST: By virtue of the powers that article 58.2 of the RGPD recognizes to each control authority, and as established in arts. 47 and 48.1 of the LOPDGDD, the Director of the Spanish Data Protection Agency is competent to resolve

this procedure.

SECOND: Before going into the substance of the matter, the formative question must be resolved.

poorly raised by the investigated entity in its pleadings brief.

The investigated entity alleges that it is completely defenseless with respect to

the facts and reasons that have supported the opening of this proceeding

sanctioning party, since they were not aware of the challenge to the file of

proceedings, that is, the appeal for reversal filed, the extension writ

of the aforementioned appeal dated February 12, 2021 and its corresponding resolution

dated February 26, 2021, in order to allege what he would have deemed convenient.

In the first place, as the reiterated jurisprudence of the Supreme Court indicates (for all

das, Judgments of the Supreme Court of October 17, 1991 and October 21,

1980) and the doctrine of the Council of State (Opinions 6,175/1997, of February 19

from 1998; 1/1998, of May 21; 3,170/1998, of July 30, and 2,301/1998, of July 10,

September, among many others), the mere omission of a procedure, even if it were mandatory

tive, it does not necessarily constitute by itself a vice of nullity in its own right.

Not even the simple omission of the hearing procedure gives rise, "always and autonomously"

tomatic", to nullity for this reason; in this regard, the Supreme Court, in Sen-

judgment of October 17, 1991, demanded "to weigh, in each case, the consequences

produced by such omission to the interested party, the lack of defense that really

originated and, above all, what could have changed the original administrative act.

in case the omitted procedure has been observed".

This is how the Council of State has ruled in its Opinions 6,175/1997, of 19

February 1998, 1/1998, of May 21, 1949/2000, of June 22, 2132/2000, of

July 20, 612/2001, of April 5, and 1,224/2001, of June 7, among others. In certain

undermined circumstances, when a careful examination of the file makes it possible to exclude

that the omission of the hearing procedure has caused defenselessness to the interested parties,

such omission may not give rise to a nullity defect.

In this sense, the Constitutional Court, in Judgment 144/1996, of September 16,

he states that "in an administrative procedure what is truly decisive

is if the subject has been able to allege and prove what he deems convenient in the as-

essential aspects of the conflict in which it is immersed".

As the Supreme Court Judgment of February 27, 1993 warns, "There is no

claim the nullity of the act because the lack of notification, even if it had existed

does not affect the validity of the uncommunicated decision, but exclusively its effectiveness

with respect to the specific recipient of the notification procedure and this on condition, for

certain, that from the omission or formal defects when practicing it, a

effective defenselessness for the same; nor would the act be null, according to

that other article invoked, when the procedure is totally dispensed with.

established procedure for making the decision; not to notify her."

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

7/8

Thus, notification constitutes a requirement for the effectiveness of administrative acts and does not

of validity, so it is unfounded to advocate the invalidity of administrative acts.

nistrative due to defects in the notification of those (For all, the Opinions of this

Advisory Council 429/2014, of September 18, or 251/2018, of July 11).

In the specific case under examination, it is known that there has been the opening of a

sanctioning procedure, without a hearing procedure having been given to the entity

investigated, by not having given notice of the motion for reversal filed, in order to

allege what he would have considered convenient, as determined in article 118 of the

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

Public Administrations (hereinafter LPACAP), which states the following:

“Article 118. Hearing of the interested parties.

1. When new facts or documents not collected must be taken into account

in the original file, the interested parties will be made clear so that, in

a period of not less than ten days nor more than fifteen, make the allegations and present

present the documents and supporting documents that they deem appropriate.

They will not be taken into account in the resolution of appeals, facts, documents or

arguments of the appellant, when having been able to contribute them in the process of

tions have not. Nor can the practice of tests be requested when your

lack of performance in the procedure in which the appealed decision was issued was

attributable to the interested party.

2. If there are other interested parties, they will be given, in any case, transfer of the resource to

that, within the aforementioned period, they allege whatever they deem appropriate.

3. The appeal, the reports and the proposals do not have the character of documents

new for the purposes of this article. Neither will those who are interested

already contributed to the file before the contested resolution was handed down.”

In view of the actions in the file, it is concluded that

in the case under examination, the investigated entity did not receive the transfer of the

replacement filed, depriving him of the possibility of formulating allegations, and

Given that such data is essential in order to defend the interested party, it is appropriate,

in accordance with the provisions of article 119 of Law 39/2015, of October 1,

of the Common Administrative Procedure of the Public Administrations, annul the

actions carried out and replace them at the time the defect occurred

procedural; however, taking into account that the alleged infringement would be

prescribed two years after its alleged commission, given that the procedure

sanctioning party in this case has not interrupted the limitation period, it is appropriate to archive this procedure, in order to comply with the principles of efficiency, rationalization and agility of administrative procedures, in accordance with article 3 of Law 40/2015, of October 1, on the Legal Regime of the Sector Public.

Therefore, in accordance with the applicable legislation and having assessed the criteria for graduation of the sanctions whose existence has been proven, the Director of the Spanish Data Protection Agency RESOLVES:

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

8/8

FIRST: FILE the sanctioning procedure PS/00332/2021 instructed to the MUNICIPAL TRANSPORT COMPANY OF \*\*\*LOCALIDAD.1 S.A.U., with CIF A46318416, for an infringement of article 32 of the RGPD, typified in article 83.4 of the GDPR.

SECOND: NOTIFY this resolution to the MUNICIPAL COMPANY OF TRANSPORTATION OF \*\*\*LOCALITY.1 S.A.U.

THIRD: COMMUNICATE this resolution to the Ombudsman, in accordance with the provisions of article 77.5 of the LOPDGDD.

In accordance with the provisions of article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reconsideration before the

Director of the Spanish Agency for Data Protection within a month from counting from the day following the notification of this resolution or directly contentious-administrative appeal before the Contentious-Administrative Chamber of the National Court, in accordance with the provisions of article 25 and section 5 of the fourth additional provision of Law 29/1998, of July 13, regulating the Contentious-administrative jurisdiction, within a period of two months from the day following the notification of this act, as provided in article 46.1 of the aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP, may provisionally suspend the firm resolution in administrative proceedings if the The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact by writing addressed to the Spanish Agency for Data Protection, presenting it through Electronic Register of the Agency [<https://sedeagpd.gob.es/sede-electronica-web/>], or through any of the other registers provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the documentation proving the effective filing of the contentious appeal-administrative. If the Agency was not aware of the filing of the appeal contentious-administrative within a period of two months from the day following the notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-171221

C/ Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

