

□ File No.: PS/00081/2022

## RESOLUTION OF PUNISHMENT PROCEDURE

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

### BACKGROUND

FIRST: Ms. A.A.A. (hereinafter, the complaining party) dated 02/04/2021  
filed a claim with the Spanish Data Protection Agency. The  
claim is directed against the CITY COUNCIL OF LARDERO with NIF P2608400D  
(hereinafter, the claimed party). The grounds on which the claim is based are  
following: the claimant states that she called the local police to report that a  
vehicle was parked in ford. A patrol showed up and completed a  
complaint bulletin, in which the personal data of the claimant was recorded  
instructing him to act as a complainant, but without giving him a copy of the  
bulletin. Required copy of the bulletin, it was sent to him, verifying that in the same  
The data of the offender, in addition to yours, are included.

Documentation provided by the claimant:

- Complaint bulletin No. XXXXX for "parking in front of a marked ford  
correctly", dated 12/16/2020. The identified vehicle appears in the bulletin  
with registration, brand and model, as well as the DNI number (NIF or DOI Document  
Identification Officer), name, surnames and address (full address) of the holder  
vehicle. The payment of the penalty is confirmed in cash. In the same bulletin appear  
the data of the claimant as "complainant", these data being the DNI, NIF, NIE or  
DOI, date of birth, name, surname and address (full address).
- Referral document of the previous bulletin digitally signed on 01/18/2021 by the  
claimed in which the text "Attached I send you the complaint bulletin XXXXX

dated December 16, 2020 requested”.

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

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

hereinafter LOPDGDD), on 03/09/2021 said claim was transferred to the party

claimed, so that it proceeded to its analysis and inform this Agency within the period

of a month, of the actions carried out to adapt to the foreseen requirements

in data protection regulations. The transfer document was collected on the day

03/30/2021 according to your acknowledgment of receipt. There is no response from the respondent.

C/ Jorge Juan, 6

28001 – Madrid

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

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

2/11

THIRD: On 06/14/2021, in accordance with article 65 of the LOPDGDD,

the claim filed by the claimant was admitted for processing.

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

of previous investigative actions to clarify the facts in

matter, by virtue of the investigative powers granted to the authorities of

control in article 57.1 of Regulation (EU) 2016/679 (General Regulation of

Data Protection, hereinafter RGPD), and in accordance with the provisions of the

Title VII, Chapter I, Second Section, of the LOPDGDD, having knowledge of the

following ends:

On 06/29/2021, information and documentation on the events was requested from the

requested, no response received. The request was collected on the day

07/01/2021, according to acknowledgment of receipt.

On 09/27/2021, the previous request is reiterated as it has not received

reply, having been collected according to the acknowledgment on 09/28/2021. Has not been received reply.

FIFTH: On 03/22/2022, the Director of the Spanish Agency for the Protection of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged Infractions of articles 5.1.f) and 32.1 of the RGPD, typified in articles 83.5.a) and 83.4.a) of the aforementioned RGPD, with a warning.

SIXTH: 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.

SEVENTH: Of the actions carried out in this procedure, they have been accredited the following:

#### PROVEN FACTS

FIRST: On 02/04/2021 the claimant filed a claim with the Agency Spanish Data Protection Agency, stating that he made a call to the police local denouncing that a vehicle was parked in a ford area. personated patrol that completed the complaint bulletin, stating the personal data of the complainant and instructing her to act as a complainant, but without making her delivery of a copy of the bulletin. Required copy of the bulletin, it was sent, noting that the offender's data appears in it, in addition to his own.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/11

SECOND: Complaint Bulletin No. XXXXX has been provided for "parking

in front of a correctly marked ford", dated 12/16/2020. in the newsletter

The vehicle identified with license plate, make and model, as well as the number of

DNI), name, surnames and address of the owner of the vehicle. Includes payment in cash

of the sanction. In the same bulletin, the data of the claimant appear in the boxes

destined to "Data of the offender", these data being the DNI, the date of birth,

name, surnames and address (full address).

THIRD: Document of submission of the previous signed bulletin is provided

digitally on 01/18/2021 by the defendant in which the text "Attached I

I send the complaint bulletin XXXXX dated December 16, 2020 requested".

#### FOUNDATIONS OF LAW

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

control authority, and according to the provisions of articles 47 and 48 of the LOPDGDD,

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

and to solve this procedure.

Yo

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

procedures processed by the Spanish Agency for Data Protection will be governed

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

regulatory provisions issued in its development and, insofar as they are not

contradict, in the alternative, by the general rules on the

administrative procedures."

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 rules regulators 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.

C/ Jorge Juan, 6

28001 – Madrid

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

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

4/11

- 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. The claimed facts are specified in that requested by the claimant a copy of the bulletin of a complaint made by the local police, they contain not only the data of the offender but also the data of the claimant, in his capacity as complainant.

### III

The RGPD deals in its article 5 with the principles that must govern the treatment of personal data and mentions among them that of integrity and confidentiality, noting:

"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").

(...)"

IV

The infraction that is attributed to the claimed one is typified in the article 83.5 a) of the RGPD, which considers that the infringement of "the basic principles for processing, including the conditions for consent under the articles 5, 6, 7 and 9" is punishable, in accordance with section 5 of the aforementioned Article 83 of the aforementioned Regulation.

The LOPDGDD in its article 71, Violations, states that:

"The acts and behaviors referred to in the regulations constitute infractions.

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that are contrary to this organic law.

And in its article 72, it considers for prescription purposes, which are: "Infringements considered very serious:

C/ Jorge Juan, 6

28001 – Madrid

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

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

5/11

1. Based on the provisions of article 83.5 of the Regulation (EU) 2016/679 are considered very serious and the infractions that suppose a substantial violation of the articles mentioned in that and, in particular the following:

a) The processing of personal data violating the principles and guarantees

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

(...)"

v

Second, it should be noted that the security of personal data

It is regulated in articles 32, 33 and 34 of the RGPD.

Article 32 of the RGPD "Security of treatment", establishes that:

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

nature, scope, context and purposes of the treatment, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical measures and

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

which in your case includes, among others:

a) pseudonymization and encryption of personal data;

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

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and evaluation of the effectiveness

technical and organizational measures to guarantee the security of the

treatment.

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

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

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

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data.

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



certification mechanism approved under article 42 may serve as an element to demonstrate compliance with the requirements established in section 1 of the present article.

4. The person in charge and the person in charge of the treatment will take measures to guarantee that any person acting under the authority of the controller or the manager and has access to personal data can only process said data following the instructions of the person in charge, unless it is obliged to do so by virtue of the Law of the Union or of the Member States”.

C/ Jorge Juan, 6

28001 – Madrid

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

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

SAW

6/11

The violation of article 32 of the RGPD is typified in the article

83.4.a) of the aforementioned 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 73, for prescription purposes, qualifies of “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 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”.

7th

From the documentation in the file, there are clear indications of that the claimed party has violated article 32 of the RGPD, when an incident of security by sending a complaint bulletin where the offender is identified along with with the complainant with breach of the technical and organizational 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 the measures technical and organizational information must be carried out taking into account: pseudonymization and encryption, the ability to ensure the confidentiality, integrity, availability and

C/ Jorge Juan, 6

28001 – Madrid

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

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

7/11

resiliency, the ability to restore availability and access to data after a incident, verification process (not audit), evaluation and assessment of the effectiveness of the measures.

In any case, when evaluating the adequacy of the level of security, particularly taking into account the risks presented by the processing of data, such as consequence of the accidental or unlawful destruction, loss or alteration of data data transmitted, stored or otherwise processed, or the communication or unauthorized access to said data and that could cause damages physical, material or immaterial.

In this same sense, recital 83 of the RGPD states that:

“(83) In order to maintain security and prevent the treatment from violating the provided in this Regulation, the person in charge or the person in charge must evaluate the risks inherent to the treatment and apply measures to mitigate them, such as encryption. These measures must guarantee an adequate level of security, including confidentiality, taking into account the state of the art and the cost of its application regarding the risks and the nature of the personal data that must be protect yourself. When assessing the risk in relation to data security, take into account the risks arising from the processing of personal data,

such as the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or the communication or access is not authorized to said data, susceptible in particular to cause damages physical, material or immaterial.

In the present case, as evidenced by the facts and within the framework of the actions E/07829/2021 the AEPD transferred the claimed on 04/26/2021 the claim submitted for analysis and reporting to this Agency of the actions carried out to adapt to the requirements set forth in the data protection regulations, without responding to the aforementioned transfer and request of information.

The responsibility of the claimed party is determined by the bankruptcy of security revealed by the claimant, since it is responsible for taking decisions aimed at effectively implementing technical measures and appropriate organizational measures to guarantee a level of security appropriate to the risk to ensure the confidentiality of the data, restoring its availability and preventing access to them in the event of a physical or technical incident. However, from the

The documentation provided shows that the entity has not only breached this obligation, but also the adoption of measures in this regard is unknown, 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 violation of article 32 of the RGPD, violation typified in article 83.4.a).

The LOPDGDD in its article 77, Regime applicable to certain categories responsible or in charge of the treatment, establishes the following:

viii

C/ Jorge Juan, 6

"1. The regime established in this article will be applicable to treatments

of which they are responsible or entrusted:

- a) The constitutional bodies or those with constitutional relevance and the institutions of the autonomous communities analogous to them.
- b) The jurisdictional bodies.
- c) The General Administration of the State, the Administrations of the autonomous communities and the entities that make up the Local Administration.
- d) Public bodies and public law entities linked or dependent on the Public Administrations.
- e) The independent administrative authorities.
- f) The Bank of Spain.
- g) Public law corporations when the purposes of the treatment related to the exercise of powers of public law.
- h) Public sector foundations.
- i) Public Universities.
- j) The consortiums.
- k) The parliamentary groups of the Cortes Generales and the Assemblies Autonomous Legislative, as well as the political groups of the Corporations Local.

2. When the managers or managers listed in section 1

committed any of the offenses referred to in articles 72 to 74 of

this organic law, the data protection authority that is competent will dictate

resolution sanctioning them with a warning. The resolution will establish also the measures that should be adopted to stop the behavior or correct it. the effects of the infraction that had been committed.

The resolution will be notified to the person in charge or in charge of the treatment, to the body on which it reports hierarchically, where appropriate, and those affected who have the condition of interested party, if any.

3. Without prejudice to what is established in the previous section, the data protection will also propose the initiation of disciplinary actions when there is sufficient evidence to do so. In this case, the procedure and sanctions to apply will be those established in the legislation on disciplinary regime or sanction that results from application.

Likewise, when the infractions are attributable to authorities and managers, and the existence of technical reports or recommendations for treatment is proven that had not been duly attended to, in the resolution imposing the The sanction will include a reprimand with the name of the responsible position and will order the publication in the Official State or Autonomous Gazette that correspond.

4. The data protection authority must be informed of the resolutions that fall in relation to the measures and actions referred to the previous sections.

C/ Jorge Juan, 6

28001 – Madrid

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

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

9/11

5. They will be communicated to the Ombudsman or, where appropriate, to the institutions

analogous of the autonomous communities the actions carried out and the resolutions issued under this article.

6. When the competent authority is the Spanish Agency for the Protection of Data, it will publish on its website with due separation the resolutions referred to the entities of section 1 of this article, with express indication of the identity of the person in charge or in charge of the treatment that would have committed the infringement.

When the competence corresponds to a regional protection authority of data will be, in terms of the publicity of these resolutions, to what is available its specific regulations.

In accordance with the available evidence of the conduct of the claimed constitutes an infringement of the provisions of articles 5.1.f) and 32.1 of the RGPD.

The RGPD, without prejudice to the provisions of its article 83, contemplates in its article 77 the possibility of resorting to the sanction of warning to correct the processing of personal data that do not conform to your expectations, when the Those responsible or in charge listed in section 1 committed any of the infractions referred to in articles 72 to 74 of this organic law.

Likewise, it is contemplated that the resolution issued may establish measures to be taken to stop the behavior, correct the effects of the infraction that had been committed and its adequacy to the requirements contemplated in articles 5.1.f) and 32.1 of the RGPD, as well as the provision of supporting means compliance with what is required.

In this same sense, it contemplates article 58 of the RGPD, in its section 2 d) that each control authority may “order the person in charge or in charge of the treatment that the treatment operations comply with the provisions of the this Regulation, where appropriate, in a certain way and within a

specified period...”.

It should be noted that the respondent has not submitted arguments to the agreement of start not knowing if it has adopted the measures of a technical and organizational nature necessary and pertinent to prevent incidents and situations such as those that have given rise to this claim will occur again in the future.

Therefore, it is necessary to point out that if the behavior is not corrected and repeated revealed in this case and that is the cause of this procedure, as well as not informing this AEPD of the measures adopted in relation to the claimed facts could proceed to the exercise of actions before the person responsible of the treatment in order to apply effectively appropriate measures in order to to guarantee the treatment of personal data and that it does not return to incurring incidents such as the one that has given rise to this claim.

C/ Jorge Juan, 6

28001 – Madrid

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

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

10/11

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 the CITY COUNCIL OF LARDERO, with NIF P2608400D, by Infractions of articles 5.1.f) and 32.1 of the RGPD, typified in articles 83.5.a) and 83.4.a) of the aforementioned RGPD, a sanction of warning.

SECOND: REQUEST the CITY COUNCIL OF LARDERO, with NIF P2608400D, so that within a month from the notification of this resolution, prove the adoption of technical and organizational measures in accordance with the regulations in



matter of protection of personal data in order to avoid that in the future incidents such as those that gave rise to the claim occur again correcting the effects of the infraction, adapting the treatment of the data of personal character to the requirements contemplated in articles 5.1.f) and 32.1 of the GDPR.

THIRD: NOTIFY this resolution to the LARDERO CITY COUNCIL.

FOURTH:

in accordance with the provisions of article 77.5 of the LOPDGDD.

COMMUNICATE this resolution to the Ombudsman,

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.

C/ Jorge Juan, 6

28001 – Madrid

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

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

11/11

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

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

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