

□ Procedure No.: PS/00053/2021

## RESOLUTION OF PUNISHMENT PROCEDURE

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

### BACKGROUND

FIRST: D. G. OF THE CIVIL GUARD (...) (hereinafter, the claimant) dated

08/07/2019 I present to the Spanish Protection Agency Act-complaint-

inspection and request for a procedure for infringement of the regulations on protection

of personal data. The claim is directed against D. A.A.A. with NIF

\*\*\*NIF.1 (hereinafter, the claimed one). The grounds on which the claim is based are, in

synthesis, that in official dependencies a person delivered documentation

found on public roads containing personal data; the holders of

the data contained in the documentation found coincide in stating that in

their domiciles, the person claimed appeared, claiming to be an authorized gas installer, and

that at the end of his work he took without consent documents corresponding to the

year 2014.

SECOND: In view of the facts denounced and the documents provided by

the claimant of which this Agency has become aware, the Subdirectorate

General Data Inspection proceeded to carry out actions for the

clarification of the facts in question.

On 10/15/2019, the claim submitted was transferred to the defendant for analysis

and communication to the complainant of the decision adopted in this regard. Likewise, it

required him to send to the determined Agency within a period of one month

information:

- Copy of the communications, of the adopted decision that has been sent to the

claimant regarding the transfer of this claim, and proof that

the claimant has received communication of that decision.

- Report on the causes that have motivated the incidence that has originated the claim.

- Report on the measures adopted to prevent the occurrence of similar incidents.

- Any other that you consider relevant.

The respondent has not responded to the request made by the Agency

Spanish Data Protection.

THIRD: On 06/08/2020, in accordance with article 65 of the LOPDGDD, the

Director of the Spanish Agency for Data Protection agreed to admit for processing the claim filed by the claimant against the respondent.

FOURTH: On 02/15/2021, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the one claimed for the alleged

C/ Jorge Juan, 6

28001 – Madrid

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

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

2/9

infringements of articles 5.1.f) and 32.1 of the RGPD, typified in accordance with the provisions in article 83.5.a) and 83.4.a) of the aforementioned RGPD.

FIFTH: Once the initiation agreement has been notified, the one claimed at the time of this

The resolution has not presented a written statement of allegations, for which reason the

indicated in article 64 of Law 39/2015, of October 1, on the Procedure

Common Administrative Law of Public Administrations, which in section f)

establishes that in the event of not making allegations within the period established on the

content of the initiation agreement, it may be considered a proposal for resolution when it contains a precise statement about the responsibility imputed, reason why a Resolution is issued.

SIXTH: Of the actions carried out in this proceeding, they have been accredited the following:

#### PROVEN FACTS

On 08/07/2019, the claimant filed with the AEPD Act-complaint-inspection and request for a procedure for infringement of the regulations on data protection of personal character, stating that in the official dependencies of the post of the G.C., a third party had delivered documentation found on public roads containing personal data; the holders of the data contained in the documentation found coincide in stating that at their homes he appeared the defendant, who claimed to be an authorized gas installer, and that at the end of his work had taken without consent documents of his ownership that coincide with the abandoned.

#### FOUNDATIONS OF LAW

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.

Yo

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.

C/ Jorge Juan, 6

28001 – Madrid

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

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

3/9

b) The facts that motivate the initiation of the procedure, its possible rating and sanctions that may apply, without prejudice to what result of the instruction.

c) Identification of the instructor and, where appropriate, Secretary of the procedure, with express indication of the system of recusal of the same.

d) Competent body for the resolution of the procedure and regulation that attribute such competence, indicating the possibility that the presumed responsible can voluntarily acknowledge their responsibility, with the effects provided for in article 85.

e) Provisional measures that have been agreed by the body competent to initiate the sanctioning procedure, without prejudice to those that may be adopted during the same in accordance with article 56.

f) Indication of the right to formulate allegations and to the hearing in the procedure and the deadlines for its exercise, as well as an indication that, in

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

initiation agreement, this may be considered a resolution proposal

when it contains a precise statement about the responsibility

imputed.

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

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

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

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

the interested".

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

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

Article 58 of the RGPD, Powers, states:

III

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

corrections listed below:

(...)

b) sanction any person responsible or in charge of the treatment with

warning when the treatment operations have infringed the

provided in this Regulation;

(...)"

The proven facts materialize in the abandonment on public roads of

documentation containing personal data allowing access to

third parties; documents obtained by the profession of the claimed, gas installer to

home, abandoning them on the public road in violation of the regulations on

Data Protection.

In the first place, article 5 of the RGPD establishes the principles that must be

govern the processing of personal data and mentions among them that of "integrity and

confidentiality”.

C/ Jorge Juan, 6

28001 – Madrid

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

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

4/9

The cited article states that:

"1. The personal data will be:

(...)

f) treated in such a way as to ensure adequate security of the personal data, including protection against unauthorized processing or against its loss, destruction or accidental damage, through the application of appropriate technical or organizational measures ("integrity and confidentiality")".

(...)

Article 5, Duty of confidentiality, of the new Organic Law 3/2018, of 5 December, Protection of Personal Data and guarantee of digital rights (hereinafter LOPDGDD), states that:

"1. Those responsible and in charge of data processing as well as all people who intervene in any phase of this will be subject to the duty of confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary of the duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will remain even when the relationship of the obligor with the person in charge or person in charge had ended of the treatment”.

The documentation in the file offers clear indications that the claimed, violated article 5 of the RGPD, principles related to treatment, in relation to article 5 of the LOPGDD, duty of confidentiality, when leaving the via public documents containing personal data with the possibility of access to third parties, documents that did not belong to him but were the property of his clients.

This duty of confidentiality, previously the duty of secrecy, must understood that its purpose is to prevent leaks of data not consented to by their owners.

Therefore, this duty of confidentiality is an obligation that falls not only to the person in charge and in charge of the treatment but to everyone who intervenes in any phase of the treatment and complementary to the duty of professional secrecy.

v

Article 83.5 a) of the RGPD, considers that the infringement of “the principles basic for the treatment, including the conditions for the consent in accordance with of articles 5, 6, 7 and 9” is punishable, in accordance with section 5 of the mentioned article 83 of the aforementioned GDPR, “with administrative fines of €20,000,000 maximum or, in the case of a company, an amount equivalent to 4% as maximum of the overall annual total turnover of the previous financial year, opting for the highest amount.

C/ Jorge Juan, 6

28001 – Madrid

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

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

On the other hand, the LOPDGDD, for prescription purposes, in its article 72 indicates:

“Infringements considered very serious:

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

particularly the following:

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

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

(...)”

Second, article 32 of the RGPD “Security of treatment”,

SAW

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)

6/9

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 32.1 of the RGPD, when an incident occurred

of security, when documents containing data are abandoned on public roads

personal data of people who had been visited at home and obtained by the

claimed as a result of his profession as a gas fitter, allowing the

access to them with breach of the established 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

C/ Jorge Juan, 6

28001 – Madrid

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

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

7/9

technical and organizational information must be carried out taking into account: pseudonymization and encryption, the ability to ensure the confidentiality, integrity, availability and 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 investigation file E/09604/2019 the AEPD transferred the defendant on 10/15/2019, the claim submitted for analysis requesting the contribution of information related to the claimed incidence, without it having been received in this body any response. Nor has it presented arguments to the initial agreement of the procedure.

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 of having notified him of the claim filed.

In accordance with the foregoing, it is estimated that the respondent would be

allegedly responsible for the infringement of the RGPD: the violation of article 32, infraction typified in its article 83.4.a).

C/ Jorge Juan, 6

28001 – Madrid

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

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

viii

8/9

In the case at hand, the sanctioning procedure is motivated because the claimed, authorized gas installer, abandoned documentation on the road containing personal data from clients, enabling its access by third parties; documentation that was collected during their home visits. The conduct of the defendant constitutes an infringement of the provisions of articles 5.1.f) and 32.1 of the GDPR.

However, as indicated in the second foundation of the RGPD, without prejudice to what is established in its article 83, contemplates in its article 58.2 b) the possibility of going to the warning to correct data processing personal data that do not meet your expectations.

In addition, the following have been taken into account, in particular: items.

- That it is a micro-SME whose main activity is not linked to the processing of personal data.
- That there is no recidivism, because the commission is not recorded, in the term of one year, of more than one infraction of the same nature.

However, in accordance with the provisions of the aforementioned article 58.2 d) of the RGPD, according to which each control authority may “order the person in charge or

in charge of the treatment that the treatment operations comply with the provisions of this Regulation, where appropriate, in a certain way and within a specified period [...].”, so the respondent is required to certifies having proceeded to the adoption of the necessary and pertinent measures of in accordance with the regulations on the protection of personal data in order to prevent incidents such as those that have occurred in the future from happening again. place to the claim, adapting the aforementioned measures to the requirements contemplated in article 5.1.f) and 32.1 of the RGPD.

It is warned that not meeting the requirements of this organization may be considered as an administrative offense in accordance with the provisions of the RGPD, typified as an infraction, being able to motivate such conduct the opening of a subsequent sanctioning administrative procedure.

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 D. A.A.A. with NIF \*\*\*NIF.1, for a violation of article 5.1.f) of the RGPD, typified in article 83.5.b) of the RGPD, a sanction of warning.

SECOND: IMPOSE D. A.A.A. with NIF \*\*\*NIF.1, for a violation of article 32.1 of the RGPD, typified in article 83.4.a) of the RGPD, a sanction of warning.

C/ Jorge Juan, 6

28001 – Madrid

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

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

THIRD: REQUIRE D. A.A.A. with NIF \*\*\*NIF.1, so that within a month from the notification of this resolution, prove the adoption of necessary measures and relevant in accordance with the regulations on data protection of personal nature in order to prevent incidents from occurring again in the future such as those that have given rise to the claim correcting the effects of the offenses committed, adapting the processing of personal data to the requirements contemplated in articles 5.1.f) and 32.1 of the RGPD.

FOURTH: NOTIFY this resolution to D.A.A.A..

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

This Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art.

48.6 of the LOPDGDD, and in accordance with the provisions of article 123 of the

LPACAP, the interested parties may optionally file an appeal for reconsideration

before the Director of the Spanish Agency for Data Protection within a period of

month from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-Administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the

Contentious-administrative jurisdiction, within a period of two months from the

day following the notification of this act, as provided in article 46.1 of the

aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the

LPACAP, the firm resolution may be provisionally suspended in administrative proceedings

if the interested party expresses his intention to file a contentious appeal-

administrative. If this is the case, the interested party must formally communicate this

made by writing to the Spanish Agency for Data Protection,

introducing him to

the agency

[<https://sedeagpd.gob.es/sede-electronica-web/>], or through any of the other

records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. Also

must transfer to the Agency the documentation that proves the effective filing

of the contentious-administrative appeal. If the Agency were not aware of the

filing of the contentious-administrative appeal within two months from the

day following the notification of this resolution, it would end the

precautionary suspension.

Electronic Registration of

through the

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

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

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