

□ Procedure No.: PS/00284/2020

## 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 claimant) on 01/21/2020 filed

claim before the Spanish Data Protection Agency. The claim is

directed against the STATE WORK AND SAFETY INSPECTION AGENCY

SOCIAL with NIF S2819013J (hereinafter, the claimed). The reasons on which the

claim are in summary: that on 10/22/2018 he addressed the aforementioned body

reporting that the company where he worked did not provide him with pay slips; the

07/14/2019 received a letter from him sending him a series of payrolls, among which

they found those of a colleague who no longer worked in the company.

SECOND: Upon receipt of the claim, the Subdirector General for

Data Inspection proceeded to carry out the following actions:

On 03/13/2020, reiterated on 06/15/2020, the claim was transferred to the defendant

presented for its analysis and it was required so that in a period of one month it

to the Agency certain 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.

There is no evidence that the respondent has responded to the requested information.

THIRD: On 09/01/2020, 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 09/24/2020, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged infringement of article 32.1 of the RGPD, typified in article 83.4.a) of the aforementioned Regulation, considering that the sanction that could correspond would be

WARNING.

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)

C/ Jorge Juan, 6

28001 – Madrid

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

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

2/11

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

FIRST: On 06/05/2019 there is an entry in the AEPD written by the claimant noting that on 10/22/2018 he addressed the respondent to inform him that the company where he worked did not provide him with payroll; on 07/14/2019 he received a letter from him in which sent him a series of pay slips, among which were those of a colleague who no longer worked in the company.

SECOND: There is a document from the Labor Inspection stating:

“In relation to the written claim presented by you, before this Inspection, against the company “B.B.B.” in which it refers to the non-delivery of payroll, I inform you:

A visit was made to the company's work center on June 10, requesting that the payroll be provided to us from the month of October 2017 until September 2018. They are attached to this document.

(...)”

Along with the claimant's payrolls, the payrolls for October, November, December and January corresponding to a third worker of the company, C.C.C.

## 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

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:

"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 regulatory norms of the procedure so provide.

C/ Jorge Juan, 6

28001 – Madrid

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

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

3/11

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.
- 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 processing operations have violated the provisions of this Regulation;

(...)

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)

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")".

(...)

Also article 5, Duty of confidentiality, of the new Organic Law

3/2018, of December 5, on the Protection of Personal Data and guarantee of the 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".

#### IV

From the documentation in the file, it is evident that the defendant, violated article 5 of the RGPD, principles related to the treatment, in relation to the Article 5 of the LOPGDD, duty of confidentiality, upon being sent a series of

pay slips, among which were those of a third party, a colleague who no longer worked in the company, allowing access to your personal data contained in them.

This duty of confidentiality, previously the duty of secrecy, must be 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

C/ Jorge Juan, 6

28001 – Madrid

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

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

5/11

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.

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.

C/ Jorge Juan, 6

28001 – Madrid

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

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

6/11

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”.

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

83.4.a) of the aforementioned RGPD in the following terms:

7th

"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 71, Violations, states 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.

And in its article 73, for the purposes of prescription, it qualifies as "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”.

viii

C/ Jorge Juan, 6

28001 – Madrid

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

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

7/11

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

that the claimed party has violated article 32.1 of the RGD, when an incident occurred

of security when transferring to the claimant the payroll of a third party in which

In addition to personal data, they include other identifying data of

labor character.

It should be noted that the RGD 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

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 RGD 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/02231/2020 the AEPD on 03/13/2020, reiterated on 06/15/2020, transferred the claim submitted to the respondent for analysis, requesting the provision of information related to the incident claimed without that any response has been received in this body.

C/ Jorge Juan, 6

28001 – Madrid

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

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

8/11

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 and, among them, those aimed at restoring the

availability and access to data quickly in the event of a physical incident or technical. However, the documentation provided shows that the entity did not not only has he breached this obligation, but it is also unknown whether he has adopted any measure despite having notified him of the claim informing him of it.

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).

Notwithstanding the foregoing, the LOPDGDD in its article 77, Regime applicable to certain categories of controllers or processors, sets the following:

IX

"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.

C/ Jorge Juan, 6

28001 – Madrid

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

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

9/11

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.

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 facts accredited in the procedure, the conduct of the claimed violates the provisions of articles 5.1.f) and 32.1 of the RGPD.

It should be noted that the RGPD, without prejudice to the provisions of article 83, contemplates in its article 77 the possibility of resorting to the sanction of warning to correct the processing of personal data that is not in accordance with your forecasts, when those responsible or in charge listed in section 1 committed any of the offenses referred to in articles 72 to 74 of this organic law.

Therefore, in accordance with the applicable legislation,

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)

10/11

FIRST: IMPOSE ON THE STATE ORGANISM LABOR INSPECTION AND SOCIAL SECURITY, with NIF S2819013J, for an infraction of article 5.1.f) of the RGPD, typified in Article 83.5.a) of the RGPD, a penalty of warning.

SECOND: IMPOSE ON THE STATE ORGANISM LABOR INSPECTION AND SOCIAL SECURITY, with NIF S2819013J, for an infraction of article 32.1 of the RGPD, a sanction of warning.

THIRD: REQUEST the STATE ORGANISM TO INSPECT WORK AND SOCIAL SECURITY, so that within a month from the notification of this resolution, accredits the adoption of measures that are necessary and pertinent 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 information of the personal data to the aforementioned measures and adapt to the requirements contemplated in article 5.1.f) and 32.1 of the GDPR.

FOURTH: NOTIFY this resolution to the STATE ORGANISM LABOR INSPECTION AND SOCIAL SECURITY.

FIFTH  
with the provisions of article 77.5 of the LOPDGDD.

: COMMUNICATE this resolution to the Ombudsman, in accordance



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

Electronic Registration of

through the

C/ Jorge Juan, 6

28001 – Madrid

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

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

11/11

day following the notification of this resolution, it would end the  
precautionary suspension.

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