



Procedure No.: PS/00129/2020

## RESOLUTION OF PUNISHMENT PROCEDURE

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

### BACKGROUND

FIRST: The claims filed by two CLAIMANTS, see ANNEX

GENERAL have entry dates 04/10 and 05/13/2019, respectively, in the Agency

Spanish Data Protection. The claim is directed against the STATE AGENCY OF

TAX ADMINISTRATION, with CIF Q2826000H (hereinafter, the claimed one). The

The reasons on which the claims are based are that in the Delegation of the State Agency

of Tax Administration of \*\*\*LOCATION.1, located at \*\*\*ADDRESS.1 of

\*\*\*LOCATION.1, it is planned to install an access and time control system for

civil servants and labor personnel based on a fingerprint system.

The complainants state that "it has begun to be required to obtain the signature of

via email." They indicate that an attempt has been made to obtain information regarding

the legality of the transfer of said data as well as the correct treatment of the same and

that the data which the employer intends to obtain constitute data especially

protected (biometric data). Such data is described in article 9.1 of the Regulation

(EU) 2016/679 of the European Parliament and of the Council of 04/27/2016 on the protection

of natural persons with regard to the processing of personal data and the free

circulation of these data (hereinafter GDPR). Article 9.2.b of the RGPD exempts

that prohibition of treatment if this is necessary for the fulfillment of obligations and the

exercise of specific rights of the person in charge of the treatment or of the interested party in the

field of labor law and social security and protection, to the extent that this is the case.

authorized by the Law of the Union of the Member States or a collective agreement with  
under the law of the Member States establishing adequate guarantees, not  
existing the mandatory evaluation of impact to the protection of data derived from said  
treatment violating the provisions of article 35 of the Regulation.

They consider that the implementation of the system is not proportional and does not comply with the law  
planned.

Complainant 1, who claims to be an official (file E/5312/2019), provides a copy of a  
email "sent to officials" of the respondent, dated 04/10/2019, entitled  
"new fingerprint identification system for access control and schedule  
in the Delegation of \*\*\*LOCALIDAD.1", in which it is reported:

- The implementation of the system and that employees will be summoned for the  
footprint taking. The date on which it is summoned appears.

-The collection system records "certain minutiae of the fingerprint, not its image",

"it is not possible to reconstruct the footprint that they characterize". "This information is stored

C/ Jorge Juan, 6

28001 – Madrid

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

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

2/12

encrypted"

-The AEAT is responsible for the treatment, indicating that article 9.2.1 b) applies as

exception for the aforementioned treatment when understanding necessary for the fulfillment of

obligations and exercise of specific rights of the person in charge or of the interested party in the

field of labor law, to the extent authorized by Union Law or

the Member States or a collective agreement under the law of the Member States

members that establishes adequate guarantees of respect for fundamental rights and

of the interests of the interested party;”, indicating that “it will not require consent, when the data processing is carried out for the fulfillment of contractual relationships of a employment, "regardless of whether it is specially protected data or not" From of taking the fingerprint as each employee must sign in the lathes, indistinctly with fingerprint or electronic DNI to enter or exit the workplace”

An ANNEX pdf document is attached: "lathe information file" although its content so it cannot be read.

-A document is also added entitled "new identification system through fingerprint to control access and schedules in the delegation of \*\*\*LOCALIDAD.1”, which contains information on legal coverage as well as “basic information on data protection”, purpose, legal basis, responsible, rights and additional information detailed by clicking the link.

-Copy of the document "Quick guide to use access control of the AEAT" that accompanies, and in addition to a graphic explanation of the position of the finger and pressure on the reader, figures that when the fingerprint is entered, “it is being checked against 1,000”, and “it ends when your ID number appears on the screen”

Complainant 2 (file E/6247/2019), adds that the electronic DNI system of each worker is used if a fingerprint mechanism error occurs and the system is running. progressively implemented throughout Spain, and which has not been previously informed to each worker of the purposes and other mandatory legal requirements for the treatment.

SECOND: Upon receipt of the claim, the Subdirector General for Inspection of Data proceeded to carry out the following actions:

The claims were forwarded to the respondent for analysis and communication to the complainants of the decision adopted in this regard. Likewise, he was required so that in the Within one month, send certain information to the Agency:

- 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 incidents from occurring

Similar.

C/ Jorge Juan, 6

28001 – Madrid

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

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

3/12

- Any other that you consider relevant.

For claimant 2, claim is transferred and responses are received from 07/29 and 10/10/2019.

It is indicated that the processes respond to the need to homogenize the systems of control of access and presence of staff to the various buildings of the Tax Agency because in some there are lathes, while in others there are only devices on the wall to record, considering the fingerprint registration system easier to use than the system of magnetic stripe card readers, which was a weaker system and generated many incidences in the management of the life cycle of the cards, including the management of the loss erase etc. With an environment of more than 26,000 employees and more than 400 buildings, the project began in 2016. This measure was selected due to a series of guarantees such as the fact that only a few details are kept at the time the transaction is registered. fingerprint. The minutiae are stored encrypted and kept in a decentralized system from where they are distributed to building turnstiles when employees are expressly authorized to access. Each employee is authorized to access the specific buildings and in the lathes of these the encrypted minutiae are downloaded so that

every time the user wants to enter or exit they can be compared with the fingerprint that is placed on the reader.

In June 2017, the start of the deployment of the solution was addressed. In a pilot phase, carried out work by the working group for adaptation to the General Regulations of Data Protection, of the security and control commission and tax informatics, reaching to the conclusion of its viability and proportionality on the basis of the legitimacy of the Tax Agency to control access and hours of its employees.

When the RGPD came into force, the existence of biometric data was already contemplated in the personnel file and in the record of treatment activities.

The implementation will be carried out gradually in all the buildings of the Tax Agency.

It has no end date.

Information and instructions were distributed to the offices where implementation was to begin of the system for its distribution among the employees with the information of the system and the guarantees of each call of the employee to go through staff to carry out the registration of the fingerprints before starting the integration the offices that have considered it prompt. They have distributed this information in a personalized way by sending an email to each employee. In ANNEX 1 attached in evidence of corporate mail with the information provided to employees used in the special delegation of \*\*\*LOCATION.1.

Regarding the questions raised:

-They consider that the information provided to the employees of the offices is complete clear and concise. The legal bases on which the access control is carried out and the guarantees are explained and the basic information required by the regulation is provided.

A link to the Tax Agency intranet was offered and more information is accessed detailed. You can consult the record of treatment activities

C/ Jorge Juan, 6

28001 – Madrid

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

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

4/12

There is no record of the request for more information about the system in the contact mailbox of queries made to the Data Protection Delegate

-Regarding the consideration of excessive treatment when there are other alternatives

emphasizes that employees are also informed that fingerprints are not stored

fingerprints but only a few minutiae or traces that are contrasted at the time of carrying out the access control. From these minutiae it is not possible to reconstruct the complete footprint and these minutiae are stored encrypted.

Provide a copy of ANNEX I that contains the same email provided by the claimant

1, of 04/10/2019 and the attached attachments.

In ANNEX II, the informative content of access to the link offered in the information.

Provides ANNEX III, a copy of the model call for fingerprint registration -which coincides with the provided by Complainant 1, "basic information on data protection

", purpose,

Legal basis, person in charge, rights and detailed additional information by clicking on

link the information is completed – informing among other extremes:

"As an alternative to identification through fingerprint readers, for cases

where technical recognition problems arise, the new system will allow

also identification by electronic DNI. In this case the identification is based on

reading the public part of this certificate, which allows you to consult the basic data of

identification (DNI number, name and surname), without the need for the worker to

provide the PIN that protects the use of certificates for authentication purposes

in electronic services or signature processes, nor will the data you may have

archived the DNI chip. In this case, the legal coverage of data processing is based on article 6.1.b) of Regulation (EU) 2016/679.”

In ANNEX II, the result of access to the link offered in the basic information on data protection, which reports in general on the processing of employee data for the fulfillment of legal obligations in terms of personnel, including among others, time control data.

In the second shipment, send a copy of the EIPD.

On 07/02 and 09/09/2019 the respondent responds to claim 1.

Provide a copy of EIPD Fingerprint

In a letter responding to the questions raised by the AEPD, it indicates that claimant 1 is a worker of the AEAT and answers the questions with the same arguments as for claimant 2.

C/ Jorge Juan, 6

28001 – Madrid

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

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

5/12

THIRD: On 09/23 and 11/25/2019, in accordance with article 65 of the LOPDGDD, the Director of the Spanish Agency for Data Protection agreed to admit for processing the claims filed.

FOURTH: On 09/30/2020, the Director of the AEPD agreed:

“INITIATE PUNISHMENT PROCEDURE a STATE ADMINISTRATION AGENCY

TRIBUTARIA, with CIF Q2826000H, for the alleged violation of article 13 of the RGPD, referred to in article 83.5.b) of the aforementioned Regulation.

For the purposes specified in the art. 64.2 b) of Law 39/2015, of October 1, of the Common Administrative Procedure of the Public Administrations, the sanction that

could correspond would be a Warning”.

FIFTH: The claim dated 10/15/2019 presents the following allegations:

Claimant 2 is not an employee of the Tax Agency and regarding claimant 1, the

04/26/2019 he was sent, like others, in the same situation, an email

Summoning you for the registration of the minutiae of your fingerprint.

They attach a copy of said mail in which they are informed of the operation of the system,

The Tax Agency is responsible for the legitimating base and the indistinct system of the

fingerprint or electronic DNI to enter and exit the work center and you are summoned to

take the fingerprint on 3/05.

A document called "lathes information file" was also attached, with a

informative content about the fingerprint system in which, in addition, it contains

basic information on Data Protection, with the person in charge, the purpose, the basis

legal treatment, recipients and additional and detailed information with a

link. This email was also received by claimant 1, including acknowledgment

of receipt of 04/26/2019.

-Adds that regarding the infraction of article 13, which specifies the principle of transparency of the

article 5.1 a of the RGPD, consider that the data has been obtained directly from the

interested and has been informed with basic information and a link to access

simple way immediately to the rest of the information. Information is abundantly contained.

in the document in which each employee is summoned to take their biometric data

since it refers that the person in charge is the Tax Agency, it also indicates the purpose of the

treatment and the possibility of exercising the rights, therefore, it is estimated that they are fulfilled

the requirements.

Provide a copy of the fingerprint EIP again.

As ANNEX 2, the information that appears by clicking on the link that appears in the emails

electronic information and communication systems for employees and that provides and extends the



information of the treatments related to the management of human resources.

C/ Jorge Juan, 6

28001 – Madrid

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

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

6/12

Provides a model call for a fingerprint registration, which contains the information section information on Data Protection and the link that expands the details and information additional.

In ANNEX 4 provides call 04/26/2020 new identification system through fingerprint.

This is an email sent on 04/26/2019 to staff of the Tax Agency, appearing among others the claimant 1. Again, the email contains information about the system, the legitimizing base and the indistinct alternative system of the electronic DNI and the pdf file called "turn information file" of which a copy is provided for reading.

The document coincides with the informative account of the system, and which contains the section on basic information on Data Protection and the link to additional information and detailed information on Data Protection, as well as a graphic scheme called "guide rapid use of access control".

It also provides a copy of the acknowledgment of receipt 04/26/2019 of the email sent to claimant 1.

SIXTH: On 04/22/2021, the Director of the AEPD agreed to change the instructor.

SEVENTH: A resolution proposal was issued with the following literal:

"That the Director of the Spanish Data Protection Agency declare the

FILE of the procedure for non-existence of infraction of the STATE AGENCY OF

TAX ADMINISTRATION, with CIF Q2826000H, for the alleged violation of the article 13 of the RGPD, in accordance with article 83.5 b) of the RGPD.”

No objections were received against the proposal.

#### PROVEN FACTS

1- In the Delegation of the State Tax Administration Agency of \*\*\*LOCATION.1,

\*\*\*ADDRESS.1 of \*\*\*LOCALITY.1, it is planned to install an access system,

time control and registration for civil servants and labor personnel based on a system of fingerprint. Gradually, the system is being implemented throughout Spain,

2-It is accredited that the claimed party sends an email to the employees, being

claimant 1 official, on 04/10/2019, entitled "new identification system through

fingerprint for access control and schedule in the Delegation of \*\*\*LOCATION.1”,

(model call for fingerprint registration) in which it is reported:

- The implementation of the system for which it is responsible for the treatment, and the next citation to each employee to take the fingerprint.

-The collection system records "certain minutiae of the fingerprint, not its image",

“it is not possible to reconstruct the trace that they characterize” and the “information is kept

C/ Jorge Juan, 6

28001 – Madrid

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

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

7/12

encrypted”

-The AEAT, indicates that article 9.2.1 b) is applied as an exception for the aforementioned treatment to understand necessary for the fulfillment of obligations and exercise of specific rights of the person in charge or of the interested party in the field of labor law.

It is accompanied by the email:

-An ANNEX pdf document: "lathe information file" entitled "new system of Fingerprint identification to control access and schedules in the delegation of

\*\*\*LOCALIDAD.1", which contains information on legal coverage as well as

"Basic information on data protection", purpose, legal basis, responsible, rights and additional detailed information. There is also a reference to a link in the that by clicking on the link information is added.

The document "Quick guide to use access control of the AEAT" with an explanation graph of the position of the finger and pressure on the reader, figuring that when the fingerprint, "it is being compared against 1,000", and "it ends when its identification number appears on the screen. DNI".

3- The respondent has a data protection impact assessment document about the collection system, fingerprint registration for the purpose of registration and control schedule.

4-The claimed person provides a copy of the same content of the email that claimant 1 provided, if Well, this mailing foresees another date of call for fingerprint collection and your name and surnames as recipient, being sent on 04/26/2020.

## FOUNDATIONS OF LAW

Yo

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

II

Biometric data is closely linked to a person, since they can use certain unique property of an individual for identification or authentication.

According to Opinion 3/2012 on the evolution of biometric technologies, "Data

Biometrics irrevocably change the relationship between body and identity, since make features of the human body machine-readable and subject to further use.

In relation to them, the Opinion specifies that different types of treatment can be distinguished noting that “Biometric data can be processed and stored in different ways.

Sometimes the biometric information captured from a person is stored and processed in

C/ Jorge Juan, 6

28001 – Madrid

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

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

8/12

raw, which makes it possible to recognize the source from which it comes without special knowledge; for example, a photograph of a face, a photograph of a fingerprint, or a recording of voice. Other times, the raw biometric information captured is treated in such a way that only certain characteristics or traits are extracted and saved as a biometric template.”

The processing of this data is expressly permitted by the RGPD when the employer has a legal basis, which is usually the employment contract itself. A

In this regard, the STS of July 2, 2007 (Rec. 5017/2003), which has understood legitimate the treatment of biometric data carried out by the Administration for the time control of its public employees, without the prior consent of the workers being required.

However, the following should be noted:

- The worker must be informed about these treatments.
- The principles of purpose limitation, necessity, proportionality and minimization of data.

In any case, the treatment must also be adequate, pertinent and not excessive in relation to said purpose. Therefore, biometric data that is not necessary for

that purpose should be removed and the creation of a database will not always be justified

biometrics (Opinion 3/2012 of the Art. 29 Working Group).

- Use of biometric templates: Biometric data must be stored as

biometric templates whenever possible. The template will need to be extracted in a way

that is specific to the biometric system in question and not used by others

controllers of similar systems in order to ensure that a person only

can be identified in biometric systems that have a legal basis for

this operation.

- The biometric system used and the security measures chosen must

ensure that it is not possible to reuse the biometric data in question for

another purpose.

- Mechanisms based on encryption technologies must be used, in order to avoid the

unauthorized reading, copying, modification or deletion of biometric data.

- Biometric systems must be designed in such a way that the authorization can be revoked.

identity link.

- You should choose to use data formats or specific technologies that

prevent the interconnection of biometric databases and the disclosure of data not

verified.

- Biometric data must be deleted when they are not linked to the purpose

that motivated their treatment and, if possible, mechanisms should be implemented

automated data deletion.

III

C/ Jorge Juan, 6

28001 – Madrid

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

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

The legitimacy for the treatment of the fingerprint for the control of the workers on the part of the employer we must look for it in article 9 and 6 of the RGPD.

Article 9 of the RGPD establishes in its sections 1 and 2.b) the following:

"1. The processing of personal data that reveals the origin racial or ethnic background, political opinions, religious or philosophical convictions, or affiliation union, and the processing of genetic data, biometric data aimed at identifying unambiguously to a natural person, data relating to health or data relating to life sexual orientation or sexual orientation of a natural person.

2. Section 1 shall not apply when one of the circumstances following:

... b) the treatment is necessary for the fulfillment of obligations and the exercise of specific rights of the person in charge of the treatment or of the interested party in the field of Labor law and security and social protection, to the extent authorized by the Law of the Union of the Member States or a collective agreement in accordance with the Law of the Member States that establishes adequate guarantees of respect for the fundamental rights and the interests of the interested party."

Article 6.1.b) of the RGPD indicates:

"1. The treatment will only be lawful if at least one of the following is met conditions:

b) the treatment is necessary for the execution of a contract in which the

The interested party is a party or for the application at the request of the latter of pre-contractual measures."

The defendant has legitimacy, based on the aforementioned regulations, to carry out the labor control of its workers, provided that it meets the requirements indicated in the Second Law Foundation.

The infringement imputed in the initial agreement of article 13 of the RGPD, was for not informing

with all the guarantees of the planned treatment, adoption of the mechanism for the control of schedule to employees by fingerprint.

This article determines the information that must be provided to the interested party in the time of collecting your data, establishing the following:

“Article 13. Information that must be provided when personal data is obtained

Of the interested.

1. When personal data relating to him is obtained from an interested party, the responsible for the treatment, at the time these are obtained, will provide you with all the information listed below:

a) the identity and contact details of the person in charge and, where appropriate, of their representative;

b) the contact details of the data protection delegate, if any;

C/ Jorge Juan, 6

28001 – Madrid

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

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

10/12

c) the purposes of the treatment to which the personal data is destined and the legal basis of the treatment; 4.5.2016 L 119/40 Official Journal of the European Union EN

d) when the treatment is based on article 6, paragraph 1, letter f), the interests legitimate of the person in charge or of a third party;

e) the recipients or the categories of recipients of the personal data, in their case;

f) where appropriate, the intention of the controller to transfer personal data to a third party country or international organization and the existence or absence of a decision to adequacy of the Commission, or, in the case of transfers indicated in the

Articles 46 or 47 or Article 49, paragraph 1, second paragraph, reference to the adequate or appropriate warranties and the means to obtain a copy of these or to the fact that they have been borrowed.

2. In addition to the information mentioned in section 1, the person responsible for the treatment will facilitate the interested party, at the moment in which the personal data is obtained, the following information necessary to ensure fair data processing and transparent:

- a) the period during which the personal data will be kept or, when it is not possible, the criteria used to determine this period;
- b) the existence of the right to request from the data controller access to the personal data relating to the interested party, and its rectification or deletion, or the limitation of its treatment, or to oppose the treatment, as well as the right to portability of the data;
- c) when the treatment is based on article 6, paragraph 1, letter a), or the Article 9, paragraph 2, letter a), the existence of the right to withdraw consent in any time, without affecting the legality of the treatment based on the consent prior to its withdrawal;
- d) the right to file a claim with a supervisory authority;
- e) if the communication of personal data is a legal or contractual requirement, or a necessary requirement to sign a contract, and if the interested party is obliged to provide personal data and is informed of the possible consequences of not provide such data;
- f) the existence of automated decisions, including profiling, to which referred to in article 22, paragraphs 1 and 4, and, at least in such cases, information about applied logic, as well as the importance and consequences provisions of said treatment for the interested party.



3. When the data controller plans further data processing

personal data for a purpose other than that for which they were collected, you will provide the interested party, prior to such further processing, information about that other purpose and any additional relevant information pursuant to paragraph 2.

4. The provisions of sections 1, 2 and 3 shall not apply when and in the to the extent that the interested party already has the information.

Regarding the imputed infraction of lack of information, it is accredited not only that has given, but rather the one that has been given before data collection, and it is estimated

C/ Jorge Juan, 6

28001 – Madrid

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

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

11/12

sufficient, adequate and extensive. It gives meaning and explains what the registration of the footprint, its purposes, and graphically the operation of the system.

Although part of the claims, both refer to the fact that he had not obtained information additional information, it must be indicated that the information provided as well as the links added are adequate and do not imply a reduction in the rights of those affected. has been offered the information contemplated by the RGD and the LOPDGDD, warning that the claimed has been preparing the gradual application of the measures with the organizational adaptations and techniques that involve the deployment of the system, so the procedure must be archived as there is no infraction.

Therefore, in accordance with the applicable legislation,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: DECLARE the FILE of the procedure due to non-existence of infraction of the article 13 of the RGD of the STATE AGENCY OF TAX ADMINISTRATION, with

CIF Q2826000H.

SECOND: NOTIFY this resolution to the STATE AGENCY OF

TAX ADMINISTRATION with the sending of the attached General Annex.

THIRD

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

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

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 one month from the day

following the notification of this resolution or directly contentious appeal

before the Contentious-Administrative Chamber of the National High Court, with

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 two months from the day following the notification of this act,

according to the provisions of 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, it may be

precautionary suspension of the firm decision in administrative proceedings if the interested party expresses

its intention to file a contentious-administrative appeal. If this is the case, the

The interested party must formally communicate this fact in writing addressed to the Agency

Spanish Data Protection, presenting it through the Electronic Registry of the

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

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

You must also transfer to the Agency the documentation that proves the filing

effectiveness 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 suspension

precautionary

C/ Jorge Juan, 6

28001 – Madrid

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

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

12/12

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-131120

GENERAL ANNEX

CLAIMANT 1- D. A.A.A.

CLAIMANT 2- D.B.B.B.

C/ Jorge Juan, 6

28001 – Madrid

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

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