

□ Procedure No.: PS/00145/2019

## RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and

based on the following

### BACKGROUND

FIRST: D.A.A.A. and Mrs. B.B.B. (hereinafter the claimants), filed the

11/20/2018 written claims before the Spanish Agency for Data Protection.

Both claims are directed against the MINISTRY OF EDUCATION and

DEPORTE DE LA JUNTA DE ANDALUCIA (hereinafter the claimed party or CONEDE), and

the reasons on which they are based are related to the

Absence control procedure for IES faculty \*\*\*IES.1 of

\*\*\* LOCATION.1 by fingerprint, stating, in short: that they have been

requested by the Secretary of the center the collection of their fingerprints for the

personal recognition for the purposes of the installation of a new control system of

assistance, within a procedure arbitrated by its management, by which

Numerous signatures have already been collected from male and female colleagues and that it could

in principle, having incurred in violation of the RGPD; that in cloister celebrated the

11/14/2018, by the Secretary and Director of the center they were informed that as of

12/01/2018, the implementation of the control of teacher absences would proceed to

through the fingerprint, as the only possible procedure despite the fact that there have been

written to both the director and the Provincial Delegation of Malaga

expressing their opposition, not having been provided with adequate information;

Likewise, legal considerations are made about the measure implemented.

requesting information on whether or not they comply with current legislation.

They provide group signatures of IES workers; letter requesting suspension

process; communication from the secretary of the IES and response from the Inspection of the Ministry of Education of the Junta de Andalucía.

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

Data Inspection proceeded to carry out the following actions:

On 01/10/2019, 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:

C/ Jorge Juan, 6

28001 – Madrid

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

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

2/16

- 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.

On the same date, the claimants were informed of the receipt of their claims and their transfer to the claimed entity.

On 02/06/2019 the DPD of the Department of Education and Sports of the Board of Andalusia communicated the responses offered to the claimants on 01/30/2019, noting that the claims had been analyzed and having obtained the

necessary information from the management of the educational center involved, informing them of the decision taken. Likewise, the AEPD was notified of the writings sent to the claimants and the writing addressed to the management of the center, as well as well as the information obtained on the causes that motivate the claims.

Likewise, the abundant information collected and related to the claims filed.

On 02/27/2019 one of the claimants submitted a brief of allegations to the response given by the DPD pointing out that in the faculty held the 11/14/2018 they were informed of the communication from the Head of Inspection favorable to the implementation of the signing method; which was given until 11/30/2018 to granting a fingerprint and having no other alternative, they were forced to deliver the same to avoid sanctions, reflecting the fact in writings attachments; in the same cloister it was reported that the DPD of the center would be the Secretary.

THIRD: On 03/25/2019, in accordance with article 65 of the LOPDGDD, the Director of the Spanish Agency for Data Protection agreed to admit for processing the claim filed by the claimant against the respondent.

FOURTH: On 11/04/2019, the Director of the Spanish Protection Agency of Data agreed to initiate a sanctioning procedure against the person claimed for the alleged infringement of article 13 of the RGPD contemplated in article 83.5.b) of the aforementioned Regulation.

C/ Jorge Juan, 6

28001 – Madrid

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

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

FIFTH: Having been notified of the aforementioned initiation agreement, the respondent submitted a written allegations on 11/18/2019 stating, in summary: that the initial agreement brought cause of the claim of the teaching staff of the educational center motivated by control schedule by fingerprint; that the DPD intervened in said claim, pointing out and transferring the decision adopted to the management of the center, informing the personal in accordance with article 13 of the RGPD; that in the start agreement the person responsible seems to be confusedly identified; that in general the responsible for time control treatment is the General Directorate of Teachers and Human Resources Management although given that the treatment that gives rise to the opening of the procedure has been decided by the management of the educational center is to said address to whom the category of data controller corresponds; that The notification of the start agreement is transferred to the address of the educational center.

The Director of the IES stated in a letter dated 12/02/2019 that he had been transferred agreement to start the procedure; that in the Cloister of 09/07/2018 reported that during the course the teacher control system would be implemented by fingerprint; in the extraordinary Senate of 10/10/2018, the teachers of the legality of the measure; On 11/05/2018, an official letter is issued by the Head of the Inspection on the measure adopted; in Cloister of 11/14/2018 it is informed of the time control system and a certificate from the installation company is provided explaining the method of operation of the fingerprint apparatus; letter from the address of center where the previous measures were reported; that on 01/16/2019 was received letter from the DPD requesting information that was sent to him and on 01/31/2019 letter of response from the DPO stating that the consent of the interested parties for the purpose of establishing said time control, although recommended that all the extremes indicated in article 13 of the GDPR.

SIXTH: On 02/03/2020 the opening of a period of practice tests began,

remembering the following:

- Consider reproduced for evidentiary purposes the claims filed by the claimants and their documentation, the documents obtained and generated by the Inspection Services that are part of the files.
- Consider reproduced for evidentiary purposes, the allegations to the agreement of start PS/00145/2019 filed by the respondent and the documentation that they accompany.

SEVENTH: On 06/10/2020, a Resolution Proposal was issued in the sense of that the defendant be sanctioned with a warning for violation of article 13 of the RGPD, typified in article 83.5 of the RGPD and in accordance with what is indicated in the Article 77.2 of the LOPDGDD.

After the period established for this purpose, the respondent has not submitted a written allegations at the time of issuing this resolution.

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

#### PROVEN FACTS

C/ Jorge Juan, 6

28001 – Madrid

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

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

4/16

FIRST. The claimants filed claims on 11/20/2018 before the AEPD, directed against CONEDE, related to the control procedure of absences of the teaching staff of the IES \*\*\*IES.1 of \*\*\*LOCALIDAD.1 by fingerprint digital.

SECOND. The Director of the educational center in writing of 12/02/2019 transferred the information required by the defendant due to the sanctioning procedure and communicated the way in which the procedure had been developed for the implementation of the access system and time control by fingerprint.

THIRD. The DPD of the defendant in writings of 02/06/2019 provided the answers offered to the claimants of the decision adopted in relation to their writings of claims filed, as well as the information collected from the Director of the IES.

The DPD pointed out that: "It should also mean here that the director of the IES, in accordance with article 132 of the Organic Law of Education, exercises the leadership of all the personnel assigned to the center, and that article 120 of the same legal text establishes the autonomy pedagogy, organization and management of educational centers, within the which can be framed this type of decisions that affect the fulfillment of teacher's schedule.

Likewise, it indicates in the aforementioned brief that "... in the present case, the interested parties possessed information, although it is not clear to us that information of all the extremes set forth in sections 1 and 2 of article 13 of the RGPD, therefore that we will go to the management of the center to recommend that you inform yourself written to the teaching staff and the administration and services staff affected by all and each of the extremes included in the aforementioned precept and so that in the future When personal damages are to be treated, proceed in this way.

On the other hand, and under the terms established in current regulations, you may request of the person in charge of this treatment the access to your personal data, the rectification or deletion where appropriate, limitation of treatment and opposition."

Claimant 1 in writing of 02/27/2019 basically provides the

FOURTH. The

documentation sent by the DPD in its previous brief and states that "The

professors and professors who subscribe to this letter, not having any alternative,

we were forced to avoid possible sanctions, to deliver the print against

of our will, this fact being reflected in a written document with

check-in center. We provide document in annex.

Record that the information cited in the minutes is provided in the faculty

of November 14 for the first time and fingerprints have been collected and it is being signed with

the digital footprint since September by a large part of the teaching staff.

It should also be noted that in that same cloister it was reported that the

Secretary of the Delegate Center for Data Protection of the Institute”.

FIFTH. ANNEX XII Diligence sent to claimant 1 by CONEDE in the

that it is pointed out that in the exercise of its functions the management of the educational center

collects teachers' fingerprints as an attendance control system,

collecting as responsible for the treatment the aforementioned Ministry.

C/ Jorge Juan, 6

28001 – Madrid

FOUNDATIONS OF LAW

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

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

5/16

Yo

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.

II

The claimed facts show the violation by the respondent of the

indicated in article 13 of the RGPD, by not informing of the planned treatment, adoption of the mechanism for the control of absences by fingerprint, with all the requirements and pronouncements established in the aforementioned article.

at the time of collecting your data, establishing the following:

This article determines the information that must be provided to the interested party

“Article 13. Information that must be provided when the personal data are obtained from the interested party.

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 all the information indicated 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 applicable;

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

IT IS

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

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

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

indicated in articles 46 or 47 or article 49, paragraph 1, second paragraph, reference to adequate or appropriate safeguards and means of obtaining a copy of these or the fact that they have been loaned.



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 data is obtained personal, the following information necessary to guarantee data processing fair and transparent

a) the period during which the personal data will be kept or, when 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 related to the interested party, and its rectification or deletion, or

C/ Jorge Juan, 6

28001 – Madrid

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

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

6/16

the limitation of its treatment, or to oppose the treatment, as well as the right to data portability;

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 the consent at any time, without affecting the legality of the treatment based on 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 providing such data;

f) the existence of automated decisions, including profiling, to referred to in article 22, sections 1 and 4, and, at least in such cases,

significant information about the applied logic, as well as the importance and

anticipated consequences of said treatment for the interested party.

3. When the person in charge of the treatment projects the subsequent treatment of

personal data for a purpose other than that for which it was collected,

will provide the interested party, prior to said further treatment, information

for that other purpose and any additional information relevant to the meaning of paragraph 2.

4. The provisions of sections 1, 2 and 3 shall not apply when and in

to the extent that the interested party already has the information.

On the other hand, article 6, Legality of the treatment, of the RGPD indicates that:

"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

interested party is a party or for the application at the request of the latter of measures

pre-contractual;

(...)"

And in article 9, Treatment of special categories of personal data,

it is established that:

"1. The processing of personal data that reveals the origin

racial or ethnic origin, political opinions, religious or philosophical convictions, or

union affiliation, and the processing of genetic data, biometric data aimed at

uniquely identify a natural person, data related to health or data

relating to the sexual life or sexual orientation of a natural person.

2. Section 1 will not apply when one of the

following circumstances:

(...)

C/ Jorge Juan, 6

28001 – Madrid

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

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

7/16

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 social security and protection, to the extent that is authorized by the Law of the Union of the Member States or a convention in accordance with the law of the Member States that establishes guarantees respect for fundamental rights and the interests of the interested;"

III

In the present case, in accordance with what is stated in the proven fact

First, the claimants filed two separate claim briefs on 11/20/2018

before the AEPD, directed against the defendant and related to the procedure of control of absences of the teaching staff of \*\*\*IES.1 of \*\*\*LOCALIDAD.1 through fingerprint, with which they were dissatisfied and about whose implantation they were not He had provided the correct information.

The Director of the educational center sent, at the request of the DPD of CONEDE, the documentation containing the development of the procedure and the measures that had been adopted to carry out the implementation of the access and control system time-river by fingerprint.

The DPD of CONEDE has provided the answers offered to the claimants about the decision adopted, in response to the requirement of the AEPD, although it is

It is true that in the aforementioned document it was recognized that although the interested parties had been

transferred information, it was not clear that they had been offered about

all the extremes contained in article 13 of the RGPD for what they recommended to

The management of the center will inform the teaching staff and the administrative staff in writing.

treatment and services affected by the measure in accordance with what is included in the pre-

mentioned concept and that in the future when personal data were to be processed

proceeded in this way.

It also indicated that the claim had been forwarded to the Directorate

General for Teaching Staff and Human Resources Management, which is listed as responsible

of the treatment activity "Control of presence inside the administrative offices

administrations, educational centers and services dependent on the Ministry of Education

management for the management of compliance with working hours and schedules" and that the General Secretary

Technical Council of the Ministry had already ruled on this matter, holding

that presence control was an important element of the principle of transparency

that should preside over the public performance and a guarantee of equality that should exist

among public employees.

First of all, reference must be made to the issue raised by the DPO

of the claimed in his letter of 11/18/2019 in relation to the person responsible for the treatment-

ment, since in addition to what is indicated in the previous paragraph, in the aforementioned writing

stated that: "... now, given that the treatment that gives rise to the opening

of the sanctioning procedure before the Ministry has been decided in terms of

its ends and means by the management of the educational center ... it is to said management that

corresponds to the category of data controller, which is based

C/ Jorge Juan, 6

28001 – Madrid

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

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

as indicated in the report of the General Directorate of Teaching Staff and Resources

Rights issued on the occasion of the claim that gives rise to this initial agreement.

Therefore, being the address of the Institute of Secondary Education "\*\*\*\*IES.1"

of \*\*\*\*LOCALIDAD.1 the person in charge of the treatment that has given rise to the agreement of

initiation of the sanctioning procedure PS/0145/2019, and as such a possible subject

saber, in accordance with the aforementioned article 70 of Organic Law 3/2018, of December 5, is

to said body to which it would proceed to notify the resolution so that it could form

formulate the allegations that it deems appropriate within the period indicated in section 4

of the agreement".

However, the documentation provided includes ANNEX XII Diligence re-

issued to claimant 1 by CONEDE on 03/04/2019, it is noted that the address of the center

The educational troop collects the fingerprint of the teachers as a control system of

assistance, with the aforementioned CONEDE appearing as responsible for the treatment and it was planned

ask the following question:

Who is responsible for the processing of your data?

Identity: Ministry of Education and Sports

Postal Address: Edif. Torretreiana. Av. Juan Antonio de Vizarrón, s/n ZIP: 41071 Seville

Data Protection Delegate: C.C.C.

DPO Contact: \*\*\*EMAIL.1

In addition, in the Personal Data Protection Guide for

Teaching Centers published by CONEDE, although it is true that in relation to

with the regulations prior to the RGPD, in its Chapter VI, Frequently asked questions about the

application of the Personal Data Protection regulations in the Centers

ters of Teaching, in relation to the registration of files and the person in charge of noti-

fy the same to the General Registry of Data Protection in the case of centers

of public education considers that “In the case of public education centers  
ca, the question arises as to whether it should be the educational center itself or the Ministry  
on which depends who should proceed to the adoption of the provision of a  
general indicated in art. 20 LOPD and its subsequent publication in the Boletín  
Official Gazette of the State or corresponding Official Gazette, as well as the consequent notification  
cation of their files in order to achieve their registration in the General Registry of Protection  
Data tion.

This issue has been resolved by the Spanish Data Protection Agency.  
in its Legal Report 143/2004, indicating the following: “... the obligation to notify  
cation will correspond to the person in charge of the file, defined by article 3 d) of the Law  
Organic 15/1999 as "Physical or legal person, of a public or private nature, or  
administrative body, which decides on the purpose, content and use of the treatment”.

To determine who has the obligation to proceed with the adoption  
of the corresponding general provision and the consequent notification of the  
treatment to the General Registry of Data Protection is essential to define  
whether if the consultant is a body incorporated in the Autonomous Administration or if the  
It has legal personality independent of it.

In the first case, the Center would be nothing more than a mere user of the file,  
whose responsibility would be the Autonomous Educational Administration, so that the obligation  
notification would correspond to the Department of Education, and should be done  
reference to the Educational Center only as the location of the file. In

C/ Jorge Juan, 6

28001 – Madrid

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

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

otherwise, the person responsible for the file would be the Center itself, corresponding to the same the notification of the treatment to the Registry of this Agency.”

In this sense, the Ministry of Education of the Junta de Andalucía has created do the ORDER of July 20, 2006, which regulates automated files with personal data managed by the Ministry of Education in the field bito of the Séneca and Pasen systems, published in BOJA no. 156, dated 11 August 2006”.

In relation to the other issues raised in the present case, there would have been to consider that the implementation and integration of a time control system based on in the fingerprint by the employer, it has to be informed to the employees of complete, clear, concise manner and, in addition, the aforementioned information must be completed with reference both to the legal bases that cover said type of control of access, as well as the basic information referred to in article 13 of the GDPR.

In the case examined, the installation of a control system based on the collection and treatment of the fingerprint of the employees, implies the treatment of your personal data since personal data is all information about a identified or identifiable natural person in accordance with article 4.1 of the RGPD.

As for the fingerprint, it is also about data that must be qualified.

two as biometric data, since in accordance with article 4.14 of the RGPD they have this consideration when they have been “obtained from a specific technical treatment”. specific, relating to the physical, physiological or behavioral characteristics of a person physical person that allow or confirm the unique identification of said person, such as facial images or fingerprint data”.

This means that in the present case, in accordance with article 9.1 of the RGPD, the specific regime provided for the special categories of

data provided for in article 9 of the RGPD.

In this sense, recital 51 of the RGPD highlights the nature

restrictive with which the treatment of this data can be admitted:

“(51) ... Such personal data should not be processed, unless it is allowed

their treatment in specific situations contemplated in this Regulation,

given that Member States may lay down specific provisions

regulations on data protection in order to adapt the application of the rules of the

this Regulation to the fulfillment of a legal obligation or to the fulfillment of

a mission carried out in the public interest or in the exercise of public powers conferred

two to the data controller. In addition to the specific requirements of that treaty

regulations, the general principles and other rules of these Regulations must be applied.

mento, especially with regard to the conditions of legality of the treatment. I know

should explicitly establish exceptions to the general prohibition of treatment

of those special categories of personal data, among other things when the in-

interested party gives his explicit consent or in the case of specific needs, in

particular when the treatment is carried out within the framework of legitimate activities by

certain associations or foundations whose objective is to allow the exercise of

fundamental liberties.

C/ Jorge Juan, 6

28001 – Madrid

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

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

10/16

And recital 52 states that:

“(52) Likewise, exceptions should be authorized to the prohibition of dealing with categories

special categories of personal data when established by Union Law or



of the Member States and provided that the appropriate guarantees are given, in order to

Protect personal data and other fundamental rights, when it is in the public interest.

co, in particular the processing of personal data in the field of labor legislation.

legislation, legislation on social protection, including pensions, and for security purposes.

ity, supervision and health alert, the prevention or control of transmissible diseases

and other serious threats to health...”

In accordance with these considerations, the treatment of biometric data re-

will want, in addition to the concurrence of one of the legal bases established in the

article 6 of the RGPD, any of the exceptions provided in article 9.2 of the RGPD.

The analysis of the legal basis of legitimacy to carry out this treatment comes

of article 6 of the RGPD, regarding the legality of the treatment, which in its section 1, letter

b) states: “The treatment will be lawful if at least one of the following conditions is fulfilled:

conditions: (...) b) the treatment is necessary for the execution of a contract in which

the interested party is a party or for the application at his request of pre-contractual measures

tuales (...)”.

By virtue of this precept, the treatment would be lawful and would not require the consent

tion, when the data processing is carried out for the fulfillment of relationships

employment contracts.

This precept would also cover the processing of employee data.

two audiences, although their relationship is not contractual in the strict sense. You have to sign-

lar that sometimes, for the fulfillment of its obligations in relation to the

public employees, the Administration must process certain data

referred to in the RGPD, in its article 9, as “special categories of data”.

cough”.

On the other hand, in the present case we are dealing with special categories of data.

personal data (art. 9.1 of the RGPD), so it will be necessary for one of the

the exceptions provided for in article 9.2 of the GPD that would allow lifting the prohibition general regulation of the treatment of this type of data established in article 9.1 of the GDPR.

At this point, special mention must be made of letter b) of article 9.2 of the RGD, according to which the general prohibition of biometric data processing does not It will apply when “the treatment is necessary for the fulfillment of obligations tions and the exercise of specific rights of the person in charge of the treatment or of the in- interested in the field of labor law and social security and protection, in the 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 establishing adequate guarantees of respect for fundamental rights and the interests of the interested”.

C/ Jorge Juan, 6

28001 – Madrid

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

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

11/16

In the Spanish legal system, article 20 of the Consolidated Text of the Statute of workers (TE), approved by Royal Legislative Decree 2/2015, of October 23, man, provides for the possibility for the employer to adopt surveillance and control measures to verify compliance with the labor obligations of its workers:

"3. The employer may adopt the measures it deems most appropriate to monitor lance and control to verify compliance by the worker with his obligations and labor duties, keeping in its adoption and application the consideration due to their dignity and taking into account, where appropriate, the real capacity of the workers with disabilities”.

And in the Basic Statute of Public Employees, approved by Royal Decree Law Legislative 5/2015, of October 30, in its article 54 in relation to the principles of behavior of public employees points out: "Unemployment of the tasks corresponding to teeth to his job will be enhanced diligently and fulfilling the day and the established schedule"

It should also be noted that the Director of the educational center, in accordance with Article 132 of the Organic Law of Education, is competent to exercise the leadership ra of all staff attached to the center.

The possibility of using systems based on biometric data is undeniable.

trics to carry out access and schedule control, although it does not seem that is or should be the only system that can be used: the use of personal cards, the use of personal codes, direct display of the marking point, etc., which may constitute, by themselves or in combination with one of the other systems available, equally effective measures to carry out control.

In any case, prior to the decision on the start-up of a control system of this type, taking into account its implications, the treatment data of a special category (biometrics), etc., would be mandatory established cer the Record of Processing Activities and carry out an impact assessment relating to the protection of personal data to assess both the legitimacy ity of the treatment and its proportionality as well as the determination of the risks and the measures to mitigate them in accordance with the provisions of article 35 GDPR.

Therefore, in the present case it must be stated that in addition to the absence ence of the Registry of Treatment Activities regulated in article 30 of the RGPD, Nor does the mandatory impact assessment regarding data protection appear regulated in article 35 of the RGPD; process linked to the principles of protection of

data by design and data protection by default intended to describe, advance and preventive manner, the processing of personal data, assess its need proportionality and manage the potential risks to the rights and freedoms to which the personal data will be exposed based on the activities of treatment carried out with them, determining the necessary measures aries to reduce them to an acceptable level of risk.

IV

C/ Jorge Juan, 6

28001 – Madrid

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

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

12/16

However, in relation to the foregoing and the need to inform tion to the interested parties, it should be noted in relation to the biometric data that the themselves are closely linked to a person, since they can use a certain unique property of an individual for identification or authentication. According to Opinion 3/2012 on the evolution of biometric technologies," Biometric data irrevocably changes the relationship between the body and identity. since they make the features of the human body readable by machines and are subject to further use."

In relation to them, the Opinion specifies that different types of treatments by pointing out that "Biometric data can be processed and stored in different ways. Sometimes the biometric information captured from a person is al-macerated and treated raw, which allows the source from which it comes to be recognized without special knowledge; for example, a photograph of a face, a photograph of a fingerprint or voice recording. Other times, raw biometric information

captured is treated in such a way that only certain characteristics or traits are extracted and they are saved as a biometric template.”

The processing of this data is expressly permitted by the RGPD when where the employer has a legal basis, which is usually the contract itself of work. In this regard, the STS of July 2, 2007 (Rec. 5017/2003), which has en-legitimate processing of biometric data carried out by the Administration for the time control of its public employees, without the need for consent. prior training of workers.

However, the following should be noted:

1. The worker must be informed about these treatments in the terms of article 13 of the RGPD.
2. The principles of limitation of the purpose, necessity, proportionality and data minimization.
3. Use of biometric templates: Biometric data must be stored as biometric templates whenever possible. The template must be extracted from a way that is specific to the biometric system in question and not used by other controllers of similar systems in order to ensure that a person can only be identified in biometric systems that have a legal basis for this operation.
4. The biometric system used and the security measures chosen must ensure that reuse of the biometric data in question is not possible for another purpose.
5. Mechanisms based on encryption technologies must be used in order to prevent unauthorized reading, copying, modification or deletion of biometric data.
6. Biometric systems should be designed in such a way that it can be revoked the identity bond.

7. You should choose to use specific data formats or technologies that prevent the interconnection of biometric databases and the disclosure of data not checked.

8. Biometric data must be deleted when they are not linked to finance. ity that motivated its treatment and, if possible, mechanisms should be implemented automated data deletion.

C/ Jorge Juan, 6

28001 – Madrid

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

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

13/16

v

Article 83.5 b) of the RGPD considers that the infringement of “the rights of those interested in accordance with articles 12 to 22”, is punishable, in accordance with the section 5 of the aforementioned article 83 of the aforementioned Regulation, “with fines administered tives of €20,000,000 maximum or, in the case of a company, an amount equivalent to a maximum of 4% of the total global annual turnover for the year previous financial agreement, opting for the highest amount”.

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

“The acts and behaviors referred to in the apartments constitute infractions.

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

The LOPDGDD in its article 72 indicates for prescription purposes: "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

entail a substantial violation of the articles mentioned therein and, in particular,

ticular, the following:

(...)

h) The omission of the duty to inform the affected party about the treatment of their personal data in accordance with the provisions of articles 13 and 14 of the Regulation (EU) 2016/679 and 12 of this organic law.

(...)"

However, the LOPDGDD in its article 77, Regime applicable to certain two categories of controllers or processors, establishes the following:

SAW

"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 State Administration, the Administrations of the communities autonomous entities and the entities that make up the Local Administration.

d) Public bodies and public law entities linked to or depending from 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.

C/ Jorge Juan, 6

28001 – Madrid

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

h) Public sector foundations.

i) Public Universities.

j) The consortiums.

k) The parliamentary groups of the Cortes Generales and the Legislative Assemblies

autonomous communities, as well as the political groups of the Local Corporations.

2. When the persons in charge or persons in charge listed in section 1

had any of the infractions referred to in articles 72 to 74 of this law

organic, the data protection authority that is competent will issue resolutions

tion sanctioning them with a warning. The resolution will also establish

as the measures that should be adopted to stop the behavior or correct the effects

cough 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

gain of which it depends hierarchically, in his case, and to those affected who had the

Interested party status, if any.

3. Without prejudice to the provisions of the preceding section, the protection authority

tion of data will also propose the initiation of disciplinary actions when

there are sufficient indications for it. In this case, the procedure and the sanctions to

apply will be those established in the legislation on the disciplinary or sanctioning system.

dor 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 corresponding Official State or Autonomous Gazette.



gives.

4. The resolutions must be communicated to the data protection authority.

tions that fall in relation to the measures and actions referred to in 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 tions 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 had committed the infringement tion.

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 the case that concerns us, it should be noted that the claim in the collection gives fingerprints for recognition and personal identification for purposes of installation of the new attendance control system, in relation to staff of the IES \*\*\*IES.1 center of \*\*\*LOCALIDAD.1, arbitrated procedure where the affected States carry out their work activity, there could have been a violation of the GDPR.

C/ Jorge Juan, 6

28001 – Madrid

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

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

In accordance with what is evidenced in the documentation provided, the conduct of the claimed constitutes an infringement of the provisions of article 13 of the RGPD.

In addition, as indicated in Basis III, prior to the decision on the implementation of a control system of this type, taking into account account its implications, the processing of data from a special category (biometrics cos), etc., it would be mandatory to establish the Registry of Treatment Activities of in accordance with article 30 of the RGPD and carry out an impact assessment re-relative to the protection of personal data to assess both the legitimacy of the treatment and its proportionality as well as the determination of the existing risks and the measures to mitigate them in accordance with the provisions of article 35 of the GDPR.

However, the RGPD itself, 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 is not in accordance with your expectations. tions, when 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 AC.

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 MINISTRY OF EDUCATION and SPORTS OF THE JUNTA DE ANDALUCIA with NIF S4111001F, for an infraction of article 13 of the RGPD, typified in article 83.5 of the RGPD, a sanction of warning.

SECOND: REQUEST the COUNCIL OF EDUCATION and SPORTS OF THE JUNTA DE ANDALUCIA with NIF S4111001F, so that within one month from the notification of this resolution, accredit before the AEPD the adoption of the measures

necessary and pertinent to correct the processing of personal data that is not  
comply with the regulations on the protection of personal data and  
prevent the recurrence of violations such as those that have given rise to the  
claim correcting the effects of the infringement, in accordance with what is indicated  
in the fundamentals IV, as well as the mandatory establishment of the Registry of  
Treatment activities regulated in article 30 of the RGPD and the Evaluation of  
Impact related to data protection regulated in article 35 of the RGPD, which  
As indicated in foundation III, it is a process linked to the principles of  
data protection by design and data protection by default, determining  
the necessary measures to reduce them to an acceptable level of risk and with the  
purpose of adapting to the requirements contemplated in article 13 of the RGPD.

THIRD: NOTIFY this resolution to the MINISTRY OF EDUCATION and

SPORT OF THE JUNTA DE ANDALUCIA, with NIF S4111001F.

FOURTH

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

: COMMUNICATE this resolution to the Ombudsman,

C/ Jorge Juan, 6

28001 – Madrid

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

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

16/16

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