 Procedure No.: PS/00131/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: D. A.A.A., on behalf of EMPLOYEES OF THE CENTER

INTEGRATED VOCATIONAL TRAINING SOMESO

(hereinafter, the

claimant), dated 11/08/2019, filed a claim with the Spanish Agency

Data Protection. The claim is directed against the MINISTRY OF

EDUCATION, UNIVERSITY AND PROFESSIONAL TRAINING OF THE GOVERNMENT OF

GALICIA with NIF S1511001H (hereinafter, the claimed). The reasons on which the

claim are: disagreement with the implementation of a control system of

access and schedule by fingerprint without having been informed to the

workers in accordance with the provisions of the regulations on the protection of

Personal data.

SECOND: Upon receipt of the claim, the Subdirectorate General for Inspection

tion of Data proceeded to carry out the following actions:

On 12/04//2019, the claim submitted was transferred to the defendant for analysis

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

required for it to send certain information to the Agency within a period of one month.

tion:

- 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 quotes.

- Any other that you consider relevant.

On 01/09/2020, the Ministry in response to the claim filed by the workers

tors states, in short, that a time control system has not been implemented

using a fingerprint as a single management system, but the use of the fingerprint

fingerprint corresponds to an alternative and voluntary modality to the biometric signature for

workers, established in accordance with data protection regulations.

And it provides: Form of consent for the treatment of biometric data and Informa-

training on the attendance management system.

THIRD: On 03/30/2020, in accordance with article 65 of the LOPDGDD, the Di-

Rector of the Spanish Agency for Data Protection agreed to admit for processing the re-

claim filed by the claimant against the respondent.

FOURTH: On 09/30/2020, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged in-

fraction of article 13 of the RGPD, typified in article 83.5.b) of the aforementioned Regulation.

and sanctioned in accordance with the provisions of article 77 of the LOPDGDD.

FIFTH: Once the initiation agreement was notified, the respondent, on 10/15/2020, presented

brief of allegations stating the following: that upon receipt of the initiation agreement

carried out the investigation of the facts requesting detailed information from the center
educational; that it is the directors of public educational centers in Galicia who
take specific organizational and management decisions that may involve the treatment
processing of personal data; that in the CIFP Someso a system has been implemented
electronic management of attendance of the personnel that provides services and due to the training
the way in which said control was carried out was not effective for the proper fulfillment
lying of the ends; that currently the electronic attendance management system
of the staff that provides service in the CIFP Someso is done by signing in a
tablet or laptop and also an optional mode, more agile and comfortable,
that works with the registration of the fingerprint, whose use is currently suspended.
actuality; that in relation to the impact assessment carried out, the Ministry is
currently addressing a global project to adapt to the protection regulations
of data, in order to prepare a record of treatment activities much
more detailed and complete than the one currently published and which will culminate in the
carrying out impact assessments of those treatments in which it is
necessary; that the duty of information was fulfilled by making available to all
personal information related to the treatment carried out; which was also required
management of the center immediate cessation in the use of the access and time control system-
fingerprint, as well as the deletion of biometric data that were
collected for such purpose and any trace thereof; that to prevent it from
situations similar to the one that is the object of this procedure, from the
Ministry is working on updating and expanding the Protocol of Pro-
Data protection in the educational field with the purpose of achieving homogenization,
as far as possible, the requirements and measures to be adopted in terms of data protection, in
hiring carried out directly by educational centers.

SIXTH: On 10/21/2020, a period of practice tests began, according to

do the following

- Consider reproduced for evidentiary purposes the claim filed by the

claimant and his documentation, the documents obtained and generated by the

Inspection Services that are part of file E/11349/2019.

- Consider reproduced for evidentiary purposes, the allegations to the initial agreement

cio presented by the claimed and the documentation that accompanies them.

SEVENTH: On 03/29/2021, a Resolution Proposal was issued in the sense that

sanction the claimant for infringement of article 13 of the RGPD, typified in article

83.5.b) of the RGPD, with a warning in accordance with article 77 of the LO-

PDGDD.

After the term legally indicated at the time of this Resolution, the re-

claimed had not submitted a pleadings brief.

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

accredited the following:

PROVEN FACTS

FIRST: The claimant submitted a document dated 11/08/2019 in the

Spanish Data Protection Agency, expressing its disagreement with the im-

planting of the access control system and schedule by means of a fingerprint by the

claimed without the workers having been adequately informed accordingly.

conformity with the provisions of the regulations on the protection of personal data.

sound.

SECOND: There is a written document dated 11/06/2019 from the claimant stating that
the workers of the vocational training center filed a claim
motivated by the following facts: that at the beginning of October he was informed
each the implementation of a time control system based on the use of the
fingerprint without being communicated the relevant information prescribed by the
GDPR; who requested the center management such relevant information as the re-
relative to the identification of the person in charge and in charge of the treatment, of the DPD, personal data
personnel made available in the elaboration of said control system, measures
technical and organizational, etc.; that the answer given by the center at two points was
generic noting that personal data is protected in accordance with the
existing legislation.

THIRD: The answer given by the educational center is recorded, by means of a letter of
10/18/2019, reporting that:

"1. The personal data of all CIFP Someso workers are pro-
fabrics in accordance with or prescribed in current legislation and are used solely and exclusively
mind to manage the internal activities of the center.

2. All contracts that CIFP Someso have signed with companies that have access to
So many files that contain data of a personal nature to two employees of the center
forum held in accordance with the requirements specified to the effect of the current legislation
tea".

FOURTH: The respondent, in writing dated 01/09/2020, indicated that the CIFP Someso did not
had “implemented a time control system using a fingerprint” as a system
single management method (as it seems to imply), but the use of the fingerprint
lar corresponds to an alternative and voluntary registration modality for workers
res” and that the necessary guarantees had been fulfilled for the start-up of
said attendance management system and provided the express consent model

prisoner for the treatment of biometric data and the information document to the

workers.

FIFTH: The respondent, in writing dated 10/15/2020, stated that: “As an initial measure,

In addition, the management of CIPF SOMESO was required to immediately cease the use of the

access control system and schedule by fingerprint, as well as deletion

of the biometric data that were collected for such purpose and of any trace of

the same…” and that “In order to prevent similar situations from being repeated in the future,

similar to the one that is the object of this procedure, from the Department is working

focusing on the updating and expansion of the Data Protection Protocol in the ambit

educational field with the purpose of homogenizing, as much as possible, the requirements

data and measures to be adopted in terms of data protection, in the contracts carried out

carried out directly by the educational centers…”

FOUNDATIONS OF LAW

Yo

The Director of the Spanish Agency is competent to resolve this procedure.

Data Protection panola, in accordance with the provisions of art. 58.2 of the

RGPD and in the art. 47 and 48.1 of LOPDGDD.

II

The legitimacy for the treatment of the fingerprint for the control of the

workers by the employer we must look for it in articles 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

ethnic or racial opinion, political opinion, religious or philosophical conviction, or affiliation

trade union membership, and the processing of genetic data, biometric data aimed at identifying

unequivocally identify a natural person, data relating to health or data relating to

you to the sexual life or sexual orientations of a natural person.

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

following companies:

(…)

b) the treatment is necessary for the fulfillment of obligations and the exercise

cio 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, in the

to the extent authorized by the Law of the Union of the Member States

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

establish adequate guarantees of respect for fundamental rights and

of 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

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

contractual.”

The defendant has legitimacy, based on the aforementioned regulations, to

carry out the labor control of its workers and as long as it meets the requirements indicated

determined in the Fifth Law Foundation.

III

The facts that motivate the claim presented and that are the subject of the proceeding

dissent materializes in disagreement with the implementation of a compliance system

access control and schedule by fingerprint without having been informed to the

workers in accordance with the provisions of the regulations on the protection of

Personal data.

These facts suppose the violation of what is stated in article 13 of the

RGPD, by not duly informing of the planned treatment in relation to the control

signing by fingerprint, in accordance with the pronouncements established in

the cited article.

time of collecting your data, establishing the following:

obtain from the interested party.

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

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

1. When personal data relating to him/her is obtained from an interested party, the res-

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.

presenter;

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 legal basis

treatment schedule;

d) when the treatment is based on article 6, paragraph 1, letter f), the interests

legitimate ses 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 decision

adequacy assessment by the Commission, or, in the case of transfers indicated

in articles 46 or 47 or article 49, paragraph 1, second paragraph, reference

lack of 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 provide the interested party, at the time the personal 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

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

cho 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 consent

at any time, without affecting the legality of the treatment based on

sado in 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 obligated

to provide personal data and is informed of the possible consequences

acknowledgments that you do not provide 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, inform

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

planned sequences of said treatment for the interested party.

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

personal data for a purpose other than that for which they were collected, you will provide

to the data subject, prior to such further processing, information about 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.

IV

In the present case, the claimant states that at the beginning of October

They were informed of the use of a time control system through

fingerprint without being duly informed in accordance with the

regulations regarding the protection of personal data. It also contributes

the letter sent to the management of the training center expressing its disagreement

and requesting information about it.

Likewise, there is a record of the response made to the claimant in which it is indicated in

two points, as it appears in the proven facts, that personal data

end of all workers are protected in accordance with current legislation and that

The companies that have access to the files containing the aforementioned data have

been celebrated with all the requirements indicated in the current legislation, and of the

It follows that neither the information transmitted nor the channel used was the most

adequate given the quality and specialty of the data that were in question,

having made a greater effort in the information and communication policy

cation about the intended treatment.

In the first place, it should be noted that the implementation and integration of a system

issue of time control based on the fingerprint by the employer, must be

informed to the employees in a complete, clear, concise manner and, in addition, the aforementioned information

training must be completed with reference to both the legal bases that give co-

opening to said type of access control, as well as to the basic information to which it does

reference in article 13 of the RGPD.

In the case examined, the response offered by the training center to the writer

submitted by the claimant, related to the aforementioned control by signing

with a fingerprint, it cannot be considered as the most suitable.

Second, the installation of a control system based on the collection

and treatment of the fingerprint of the employees implies the treatment of their data

personal since personal data is all information about a person

physical identified or identifiable 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 and in accordance with article 4.14 of the RGPD have this

consideration when they have been “obtained from a specific technical treatment”.

co, relating to the physical, physiological or behavioral characteristics of a natural person

that allow or confirm the unique identification of said person, such as images

facial expressions or dactyloscopic data”.

This means that, in accordance with article 9.1 of the RGPD, in the pre-

present, 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.

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 of special categories will require, in addition to the concurrence of one of the legal bases cas established in article 6 of the RGPD, some of the exceptions provided in the 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, on occasions, 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, and as highlighted in recital 51 of the same RGPD,

to the extent that the biometric data are of a special category in the cases

of biometric identification (art. 9.1 RGPD), it will be necessary that one of the

the exceptions provided for in article 9.2 of the RGPD that would allow the prohibition to be lifted.

general regulation of the treatment of these types of data established in article 9.1.

At this point, special mention must be made of letter b) of article 9.2 of the

RGPD, 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".

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"

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: thus, the use of person-cards

them, the use of personal codes, the direct visualization of the marking point,

etc., which may constitute, by themselves or in combination with any of the other

available systems, 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 and taking into account its implications,

development of biometric data aimed at uniquely identifying a physical person

it would be mandatory to carry out an Impact Assessment related to the protection

of personal data to evaluate both the legitimacy of the treatment and its

proportionality such as the determination of the existing risks and the measures to

mitigate them in accordance with the provisions of article 35 RGPD.

v

Biometric data is closely linked to a person, given

that they can use a certain unique property of an individual for their identification.

cation or authentication.

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

“Biometric data irrevocably changes the relationship between the body and identity.

ity, since they make the features of the human body legible by means of

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:

O The worker must be informed about these treatments.

O The principles of limitation of the purpose, necessity, pro-

proportionality and data minimization.

In any case, the treatment must also be adequate, pertinent and not ex-

cessive in relation to said purpose. Therefore, biometric data that is not necessary

necessary for that purpose should be abolished and the creation of

a biometric database (Opinion 3/2012 of the Art. 29 Working Group).

O Use of biometric templates: Biometric data should 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.

O 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.

O Mechanisms based on encryption technologies should be used in order to

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

O Biometric systems should be designed in such a way that they can be revoked

the identity bond.

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

prevent the interconnection of biometric databases and the disclosure of data

not checked.

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

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

automated data deletion.

SAW

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-

ment (EU) 2016/679 and 12 of this organic law.

(…)"

7th

However, the LOPDGDD in its article 77, Regime applicable to certain

two categories of controllers or processors, establishes the following:

"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

tions 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 de-

pending 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.

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

ferred 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 and as indicated previously, the presen-

sanctioning procedure evidences that the defendant has not adequately informed

mind in relation to the control of access to the facilities of the training center

through a fingerprint system, as an alternative and voluntary system to that of the

signature.

In accordance with the evidence available to said conscientious conduct,

It constitutes an infringement of the provisions of article 13 of the RGPD.

The RGPD, without prejudice to the provisions of its article 83, contemplates in its article

Article 77 the possibility of resorting to the sanction of warning to correct the treat-

processing of personal data that do not conform to their expectations, when they are answered

officers or managers listed in section 1 committed any of the offenses

tions referred to in articles 72 to 74 of this organic law.

However, the respondent has stated that the address of the

CIPF SOMESO the immediate cessation of the use of the access and time control system

by fingerprint, as well as the deletion of the biometric data that were collected.

constructed for such purpose and of any trace thereof and, furthermore, that the

center of the need to notify the data protection delegate of the Conse-

would require the provision of contracting any service or supply that might entail

have an innovative treatment of personal data of students, their families,

lias or the staff of the center itself, so that the data protection delegate

could advise in a timely manner on the legality of said treatment and supervise the

GDPR compliance. Likewise, it has been pointed out that in order to prevent them from repeating

In the event of similar situations, the Ministry is working on updating

and expansion of the Data Protection Protocol in the educational field for homo-

Generate, as far as possible, the requirements and measures to be adopted in terms of protection of

data, in the contracts carried out directly by the educational centres.

On the other hand, the respondent has also considered relevant to point out that:

- Is fully aware of the special sensitivity of personal data

treated by some of its services, as well as by the teaching centers dependent on

teeth of the same, and especially those related to minors.

- That, among said adaptation works, are:

- The review and analysis of each of the treatments carried out,

its purposes and bases of the treatment, which suppose the corresponding action

lization of the record of treatment activities on the already published to the

entry into force of the LOPDGDD, and which will be disseminated through the website

corporate page of the Xunta de Galicia

- Review and update of informative clauses for people

stakeholders (adequacy of the legitimizing bases of the special treatment-

mind regarding the applicability of consent) and the necessary

to regulate the relationship responsible-processor or between correspondents

liable in your case.

- Carrying out the corresponding risk analyzes and evaluations of

impact on data protection.

- The provision of training sessions on personal data processing.

personal addressed to the staff of the Ministry.

- Once the adaptation work has been completed, the Delegate for the protection of

data of this Ministry will send an informative circular in this regard addressed to

users of the information system in which the state of di-

Many works, the main documentation and regulations on the matter.

Therefore, in light of the foregoing, it is considered that the response of the claimant

has been reasonable and his diligent action, correcting the incident not pro-

urging the adoption of additional measures, having been accredited the sus-

pension of the access control system by means of a fingerprint, as well as the erasure

of the biometric data that were collected, adopting other types of quality measures

technical and organizational nature in accordance with the regulations on protection

data previously indicated and prevent situations from occurring again.

tions such as the one that gave rise to this claim, which is the main purpose of

the procedures regarding those entities listed in article 77 of the

LOPDGDD.

Therefore, in accordance with the applicable legislation and after assessing the graduation criteria

tion of the sanctions whose existence has been proven,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE THE MINISTRY OF EDUCATION, UNIVERSITY AND TRAINING

PROFESSIONAL REGION OF THE GALICIA GOVERNMENT, with NIF S1511001H, for an in-

fraction of article 13 of the RGPD, typified in article 83.5.b) of the RGPD, a sanction

warning in accordance with the provisions of article 77 of the LO-

PDGDD.

SECOND: NOTIFY this resolution to the DEPARTMENT OF EDUCATION,

UNIVERSITY AND PROFESSIONAL TRAINING OF THE GALICIA GOVERNMENT, with NIF

S1511001H.

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 LPA-

CAP, 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

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

contentious-administrative case before the Contentious-administrative Chamber of the Au-

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 Jurisdiction

Contentious-administrative diction, within a period of two months from the day following

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 LPA-

CAP, the firm resolution may be provisionally suspended in administrative proceedings if the

The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact by

writing addressed to the Spanish Agency for Data Protection, presenting it through

Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registers provided for in art. 16.4 of the city

tada Law 39/2015, of October 1. You must also transfer to the Agency the documentation

certifying the effective filing of the contentious-administrative appeal. Yes

the Agency was not aware of the filing of the contentious-administrative appeal

nistrative within two months from the day following the notification of the pre-

This resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es