 File No.: PS/00052/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant) on 07/03/2020 filed

claim before the Spanish Data Protection Agency (AEPD) The claim

is directed against the CONSORTIUM FOR THE CONSTRUCTION, EQUIPMENT AND

OPERATION OF THE SPANISH HEADQUARTERS OF THE EUROPEAN SOURCE OF

SPALATION NEUTRONS with NIF G95455473 (hereinafter, the claimed one).

The defendant declares that he was a union delegate, but no longer provides his services for

the claimed. The grounds on which the claim is based are that, since November

2019, the respondent has implemented a presence control system in the company,

hourly signing by biometric fingerprint recognition. It was distributed among the employees

two a document, identified as 1, where consent is required for the

processing of biometric data and requests that it be determined whether the person claimed has acted

tuated in accordance with current legislation.

Provides:

- DOCUMENT 2, delivered by the respondent, informative, entitled

“LEGAL ASPECTS OF SIGNING WITH BIOMETRIC READERS OF

ROBOTICS (company with which they contracted the system) WHAT SHOULD BE

NOTICES TO STAFF”, on the characteristics of the systems

ROBOTICS biometrics, with the literal:

“From the moment a user puts their finger on the terminal reader,

generates an identification number. This number is the one that is stored in the

memory of the terminal and the one that is distributed to the other terminals. This same

This number is used to compare whether the fingerprint corresponds to a user or not. East

number has no value outside the ROBOTICS terminals, nor is there any way

one of obtaining an image from it, that is, it is not reversible"

-"The AEPD determines that these data have the condition of a personal nature of

special category." "The data stored in ROBOTICS systems does not

contain no particular aspect of personality, limiting their function to identifying

to a subject when the information is linked to it."

-"Regarding the need for the interested party to give their consent or to be able to

oppose the processing of your biometric data, it should be noted that article 7 of the

RGPD- Regulation (EU) 2016/679 of the European Parliament and of the Council of

04/27/2016 regarding the protection of natural persons with regard to

processing of personal data and the free circulation of these data (hereinafter,

RGPD);-requires the consent of the interested party for any treatment of their

personal data including those of a special category. "The tratment of

biometric data is covered by article 9.2 b) of the RGPD when obtaining the

explicit consent of the worker or be necessary for the fulfillment of

obligations and the exercise of specific rights of the data controller -

company -in the field of labor law and security."

-"Based on article 20.3 of the Royal Decree approving the Law of the Statute of

Workers, the company may adopt the most appropriate measures of surveillance and

control to verify compliance by the worker with the obligations and duties

employment, in which the use of biometric data to control access to dependencies

of the company is legitimate and not disproportionate to the purpose of the treatment.“

“Based on article 6 of the RGPD, the treatment will be lawful through the consent

of the interested party -employee- or if the treatment is necessary for the execution of a

contract to which the interested party is a party.

“It is necessary for the company to inform its employees of all of the above

prior to the use of such systems in order to facilitate such communication.

ROBOTICS puts at your disposal an informative note that companies should

deliver and have your workers sign at the time of digitizing their fingerprints

fingerprints in order to be able to prove before an inspection that the workers gave

your express consent to the processing of biometric data”.

“In conclusion, the biometric data of the ROBOTICS systems allow the

unequivocal identification of individuals without violating their rights and freedoms

fundamental.”

-DOCUMENT 3, delivered by the company and signed by ROBOTICS, entitled

"SUPPLIERS CONTRACTED BY ROBOTICS WITH ACCESS TO DATA" that

contains three companies “that have access to our data”, one of them

MICROSOFT IRELAND OPERATIONS LIMITED “SaaS service”, and two companies

Spanish: support ticket management service, and “e-learning” training platform.

-Copy of email from the claimant to the company, dated 10/2/2019, stating-

dole that according to a query that he made, the AEPD does not consider it accurate or

Consent is necessary in the implantation of the fingerprint as a system of

signing, related to the fulfillment of obligations.

He adds that the data is biometric, requesting to be informed of the treatment of his

data, including impact assessment. Accompanies the consultation document signed

approved by the AEPD on 09/30/2019 in which, among other statements, it is stated that in

the case presented, "the employer should not seek the consent of the workers

agents to proceed with said treatment but that this will be based on a legitimate basis

different dora…"

-DOCUMENT 1, entitled: "Model consent document for trafficking-

biometric data collection", which is a form to be completed and signed by employers.

employees that contains a declarative part, and an informative part, being considered as

"conformity test". The document declares that it "expressly consents" "to digitize

Use the fingerprint in order to carry out the control of the presence of the

employees through biometric recognition in which "the system through authentication

Biometric authentication does not store an image of my fingerprint, but a number generated by

from this." "I have been informed that the number stored from my fingerprint

will remain active in the system for the duration of my employment relationship "also that

They will not keep a complete image of the fingerprint but only a created number.

do from the footprint. Said number does not allow to reconstruct the footprint." In section

of information is indicated in legitimacy: "consent of the interested party". The document

to figure dated 01/7/2020, receipt note, indicating "I do not consent. I request the sub-

pressure of all my personal data from any registry, database or similar

of the company or third parties to whom said data has been transferred. "

SECOND: Within the framework of the actions carried out by the Subdirectorate General

of Data Inspection, the claim is transferred dated 08/7/2020, with the literal:

“ FACTS GIVING RISE TO THE CLAIM

:

The complainant states that the company Consorcio ESS Bilbao ORG has implemented

a presence control system using a fingerprint that does not comply with the

parameters established by the data protection regulations.

RELEVANT DATA:

The documentation submitted with the claim is provided.

It must be reported, with what is requested in the following paragraph and within the same period,

on the Impact Assessment carried out and all the information provided to the

workers.

Within a maximum period of one month, from the receipt of this letter, you must

analyze the claim and send this Agency the following information:

Report on the causes that have motivated the incidence that has originated the

1. The decision made regarding this claim.

2. In the event of exercising the rights regulated in articles 15 to 22 of the

RGPD, accreditation of the response provided to the claimant.

3.

claim.

Four.

Report on the measures adopted to prevent incidents from occurring

similar, dates of implementation and controls carried out to verify their effectiveness.

5. Any other that you consider relevant.”

On 09/08/2020, a response is received, stating:

1) They signed a CONTRACT on 05/24/2019 with the company ROBOTICS, SA. attach

copy of the document called “proposal”, “PROJECT FOR THE IMPLEMENTATION OF

THE “VISUALTIME” SaaS SOLUTION for the ESS Bilbao, offer. stand out as

The following points are most significant:

-The model on which the "VisualTime" solution offered is based is that of comprehensive service

o SaaS, “software as a service” that includes all the necessary services for the

commissioning, installation of hardware components, activation of the

“VisualTime” license, web access to their supervisors for the exploitation of the information

training and treatment, export and import of data through web access and

continuity and maintenance service to respond to requests and queries, resolve

Incidents and periodic software updates, backup copies and Protection

of data.

-The model works on a "cloud" platform with the advantages of being in the cloud.

-There are four terminals.

-It appears in the license agreement for use and services, that "VisualTime" is the application

in which the data is stored. ROBOTICS, signed the accommodation contract or

cloud computing services for this operation with MICROSOFT IRELAND OPE-

RATIONS LTD (MIO) for the correct provision of the service object of the license, which

is also considered in charge of treatment with regard to the operation

of the server. The client expressly authorizes the supplier to subcontract with MIO the

cloud computing hosting services for the correct provision of the service object of

license, which implies the access and processing of the data contained in the license file.

ownership of the client called "human resources" by both third parties, granting

the supplier the power to contractually require the subcontractor to implement

in its facilities of the same security measures by the implemented pre-

seen all of them in the RGPD.

-ANNEX III, “data security”, “VisualTime”” SAAS informs that, among other information,

information, that ROBOTICS will process personal data related to the identification

of the client's employees, employment data necessary to offer the solutions

contracted and biometric data. The respondent states that he has a certificate that

complies with the requirements of the National Security Scheme,

-There is an ANNEX IV dedicated to DATA PROTECTION (page 50 of the pdf "project

implantation”). It is indicated that the supplier, ROBOTICS, is in charge of the treatment

treatment and access to the data- property of the client as responsible for the treatment-

according to the client's instructions, always in reading query mode and other references

references to security issues that must be met.

2) It states that ROBOTICS "instructed us that it does not proceed to a storage of

the fingerprint on your part and that the “VisualTime” application does not carry out a treatment

storage of particularly sensitive personal data, given that the terminals of RO-

BOTICS do not store an image of the employee's fingerprint, only a number.

A many-digit number that is generated from the fingerprint. It is completely impossible

It is possible to create a photograph or re-fingerprint an employee from that

number."

For all these reasons, it was not considered necessary to carry out an impact assessment on

data protection, since it was not within the assumptions collected in

Art. 35 of the RGPD.”

3) Provide a copy of DOCUMENT 5.4. of "personal data protection security"

les”, of 06/10/2019, version 01 in which in “5. Processing registry” “they do not identify

fy or describe what they are, mentioning the legal references, a section 9 of

"risk analysis" with legal references, categorizes the types of risks and the

general risk assessment system for the different treatments that lead to

cape. Section 10: "Impact Assessment", lists the legal regulations and acts

res that participate in it. (archive, part two, p. 35/77). of "appointment of

data protection delegate” DOCUMENT 5.4.2. with communication to the AEPD

on 12/2/2019 and a "Final report on the implementation process of the Pro-

Data Protection” dated 12/2/2019 with two pages.

4) Considers that the treatment of these data “is necessary for the fulfillment of

obligations and the exercise of specific rights of the ESS Bilbao Consortium in the

field of labor law and social security and protection, in accordance with

what is established in RD Law 8/2019 of March 8, which establishes the obligation

companies to implement a system for recording working hours that must be included

include the specific start and end time of the working day for each job.

jador Despite this, the ESS Bilbao Consortium decided, based on principles of transparency

request prior to its implementation the consent of all employees.

beef. All workers signed their consent.”

The ESS Bilbao Consortium “made the necessary communications to the entire workforce” (5.2

of the document) which includes emails reporting on 16, 23 and

09/27/2019 from:

-Implementation of the time control system and registration of the working day. From

On October 1, the financial system will be launched as a test for a month.

chajes “VisualTime” and “we hope to launch the system to the entire staff at 1

of November".

- You are sent:

-The document issued by ROBOTICS in relation to compliance in ma-

RGPD ("legal aspects of the signing with biometric readers of ROBOTICS

that must be communicated to the staff.

-"Workday instructions and schedules for ESS Bilbao agreed with the re-

representatives of the workers, as well as the document that certifies compliance

of the RGPD by the company Robotics (supplier of the clocking system)."

-Document to fill out on consent for data processing

biometrics "Behind you have detailed information about the PD in terms of time control-

river respects".

The decision on the implementation of this signing system was preceded by a

period of consultations with the representatives of the workers". They provide:

-Copy of minutes of meetings held on 05/08, 09/23 and 11/18/2019 (DOCUMENTS

5.3.1, to 5.3.3). (part two of the file presented, page 14/77)

- Attached as DOCUMENT 5.3.4. and among the documentation a list was delivered-

of suppliers contracted by ROBOTICS with access to data (it appears in DOCU-

MENT 5.1.4.)

5) In file part two, (page 71/77), copy of the report of AUREN CONSULTORES

SP, SLP of 09/04/2020 on the progressive process of implantation of the biome-

tricho indicates:

“To assess the scope of the data processing carried out by ROBOTICS, it is analyzed

together with the Consortium:

-The guarantees offered by ROBOTICS in relation to the activities to be carried out

-Degree of compliance with the RGPD and information security issues.

-Characteristics of the technical system used for data processing

fingerprint, which is done through the application marketed by ROBOTICS "Visual-

Time.”

“Taking into consideration the information collected from the supplier ROBOTICS (designation

Nation of DPD, certification in the National Scheme of Security, service contract

services with a description of security measures, etc.), and the documentation provided in

In relation to the "VisualTime" application (attached document), it was considered that the pro-

ROBOTICS veedor offered guarantees in matters of data protection and security of

the information, and that the marketed application "VisualTime" did not carry out a treatment

storage of particularly sensitive personal data. For all these reasons, it was not considered

necessary to carry out an impact assessment on data protection, since it does not

was within the assumptions contained in art. 35 of the RGPD”.

6) Provides in section 5.1 (file part one, page 16/73) “compliance information

data protection regulations by ROBOTICS”, which is made up of:

- already mentioned document “legal aspects of signing with biometric readers”

ROBOTICS issues that must be communicated to the staff”

- graphic scheme of “Terminals-Communications scheme” with the phases:

- Registration of fingerprint: “the registration of the new fingerprint is carried out in the terminal that generates and stores

have a hash dinner.” An arrow that appears on a screen indicates” “VisualTime” does not store

a fingerprint image only stores the generated hash”. Another arrow out

to another drawing indicates: “the validation of the fingerprints is carried out in the terminal itself that

compares the hash stored in the terminal and sends "VisualTime" a user ID

according to its validity and type.

-Fingerprint distribution: a screen that indicates “VisualTime” only trans-

submits the hash to authorized endpoints.

-Elimination of traces, in a drawing of the screen figure “VisualTime” eliminates the da-

terminals according to authorization of the employee or permanent dismissal

7) Provide a copy of the ROBOTICS information sheet entitled “Information note about

the protection of personal data in the terminals”: “The terminals of ROBOTICS

they do not store an image of the biometric system they use to identify employers.

used, they only generate a multi-digit number from the biometric data.

co used. It is completely impossible to create a picture or get the

biometric data of an employee from said number.

For practical purposes, this means that every time you identify yourself by means of a

biometric data in the terminal, a number is generated. The program then compares if

this number corresponds to an employee or not in the same way that it would with a

card-."

THIRD: The Director of the Spanish Data Protection Agency agreed to

12/18/2020 admit the claim filed by the claimant for processing.

FOURTH: On 09/16/2020, a letter was received from the claimant specifying

The complaint consists of two parts:

-The first refers to the use of biometric data, which the company says not al-

macena.

The second part refers to the fact that the company informs the workers of

that your personal data will be accessible by the installation company, but not

such data can also be accessed by other companies, such as MICRO-

SOFT.

It indicates that the company has four offices (2 in Bizkaia, 1 in Álava and another in Madrid) and

that in all four the same data treatment is given to all employees.

On the other hand, "I would like to expand the complaint: The company for some years has

started processing payroll with an external company." "Since the information

that they give to said company I believe that it includes personal data of a protected category

(salary, identity, social security number, DNI...) I think I should tell the employees

two that said data will be shared with third parties. It never has. I know

I have personally pointed it out and they have done nothing to fix it."

FIFTH: On 04/19/2021, the Director of the AEPD agreed to initiate against the

claimed, sanctioning procedure of warning for the alleged infringement

of article 35 of the RGPD, in accordance with article 83.4.a) of the RGPD.

SIXTH: On 05/04/2021, allegations were received from the respondent, stating:

-In the election of the treatment manager for the day registration system

of the employees had diligence to choose him, "examining the risks

that implied the use of said registry" "providing itself with technical measures and

appropriate organizational structures", "having an ISO 27001 certification, they provide

document 1

- "Understanding now the criteria of the AEPD on the treatment of biometric data

specially protected and the need to prepare an Impact Assessment on the

case that concerns us here, we will proceed to carry out the same as soon as possible

possible."

-Provides documentation that has already been previously provided:

-ANNEX III, "data security", "VisualTime"", which is part of the contract

with ROBOTICS, (3/53).

-Consent document.

-Security document - data protection. (version still 01, of

06/10/2019) that appears as referred to in document 5.4

SEVENTH: On 12/13/2021, a resolution proposal is issued with the following

literal:

“FIRST: That by the Director of the Spanish Agency for Data Protection,

sanction CONSORTIUM FOR THE CONSTRUCTION, EQUIPMENT AND

OPERATION OF THE SPANISH HEADQUARTERS OF THE EUROPEAN SOURCE OF

SPALATION NEUTRONS, with NIF G95455473, for an infringement of the

article 35 of the RGPD, typified in article 83.4 a) of the RGPD, and for the purposes of

prescription, in article 73.t) of the LOPDGDD, with a warning.

SECOND: That the Director of the Spanish Data Protection Agency

proceed to impose CONSORTIUM FOR THE CONSTRUCTION, EQUIPMENT AND

OPERATION OF THE SPANISH HEADQUARTERS OF THE EUROPEAN SOURCE OF

NEUTRONS BY SPALATION, in the term that is determined, the adoption of the

necessary measures to adapt to the personal data protection regulations

the treatment operations it performs, with the scope expressed in the

Foundations of Rights of this proposed resolution.”

On 12/22/2021, allegations are presented stating that upon receiving the

proposal have ceased to use the tool for the use of biometric data

as time control, adopting the control system through identification cards.

Provide a copy of the order for proximity cards, delivery date 12/27/2021.

Request that no penalty be imposed.

EIGHTH: Of the actions carried out in this procedure and of the

documentation in the file, the following have been accredited:

PROVEN FACTS

1) The respondent decided to start in 2019 the progressive implementation of a system

presence control, hourly signing by biometric fingerprint recognition.

2) The respondent bases the legality of said treatment on at least three reasons:

-“It is necessary for the fulfillment of obligations and the exercise of specific rights.

objectives of the ESS Bilbao Consortium in the field of labor law and security and

social protection”, (article 6.1b) of the RGPD, “in accordance with the provisions of the

RD Law 8/2019 of March 8, which establishes the obligation of companies

sas to implement a day registration system that must include the specific time

of start and end of the working day of each worker” (6.1.c) of the RGPD).

Despite this, the ESS Bilbao Consortium decided, based on principles of transparency, to request

require prior to its implementation the consent of all workers

(6.1.a of the RGPD), indicating that all workers signed their consent, if

Well, the claimant's does not appear more than the one I received on 01/7/2020, with the note of "not con-

I feel".

3) The respondent informed the staff of the system to be implemented. It is also stated that
They held meetings with the workers' representatives. Declare the claim
do that the system was going to be implemented in test mode as of 10/1/2019 and to
the entire staff as of 11/1/2019.
4) The respondent provides a copy of the treatment order contract signed on
05/24/2019 with ROBOTICS. ROBOTICS accesses data of the claimed person stored
in the “human resources” file in accordance with the instructions of the person claimed. Them-
These data are stored in the VISUALTIME application, a comprehensive software solution, in the
that all the underlying infrastructure, middleware, software, and data of the
applications are located in the provider's data center. For storage-
storage of the data, ROBOTICS has signed a hosting contract of "cloud
computing” with MICROSOFT IRELAND OPERATIONS LTD which is considered sub-
charged with the treatment regarding the operation of the server.
5) The system for registering and using the fingerprint of the employees, in accordance with the
ROBOTICS document, called "LEGAL ASPECTS OF SIGNING WITH
ROBOTICS BIOMETRIC READERS THAT MUST BE COMMUNICATED TO THE
PERSONAL” consists in that: “A number generated from characters is stored
physical characteristics of a person. “From the moment a user puts their finger
in the terminal reader (they have four), an identification number is generated.
This number is the one that is stored in the terminal's memory and the one that is distributed to
the other terminals. This same number is the one used to compare if the fingerprint
corresponds to a user or not. This number has no value outside the terms.
ROBOTICS terminals, nor is there any way to get an image from it.
that is, it is not reversible”.
Regarding the registration of the fingerprint, the respondent indicated that "it is carried out in the terminal that
generates and stores a hash”. “VisualTime” does not store a fingerprint image

it only stores the generated hash". "The validation of the fingerprints is carried out in the

own terminal that compares the hash stored in the terminal and sends to "VisualTime"

a user ID according to its validity and type."

-Fingerprint distribution: a screen that indicates "VisualTime" only trans-

submits the hash to authorized endpoints.

6) The claimed party has a generic security document, version 1, of

06/10/2019, which he provided in his response to the transfer to the claim and in allegations

to the proposal, which contains generic indications for the safety of treatments

lies. The respondent does not have the project impact assessment document.

Data protection of the biometric data that it processes in relation to its control purpose

schedule.

7) After the proposed resolution, the respondent stated that the treatment had ceased.

fingerprinting, changing to the proximity card system.

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

process.

II

The scope of application of the RGPD extends its protection, as established by its

article 1.2, to the fundamental rights and freedoms of natural persons and, in

particular, your right to the protection of personal data, defined in its article

4.1 as “all information about an identified or identifiable natural person (“the

interested"); An identifiable natural person shall be deemed to be any person whose identity

can be determined, directly or indirectly, in particular by means of an identifier,

such as a name, an identification number, location data, a

online identifier or one or more elements of physical identity,

physiological, genetic, psychic, economic, cultural or social of said person.”

Biometric data is defined by article 4.14 of the GDPR:

"biometric data": personal data obtained from technical processing

specific, relating to the physical, physiological or behavioral characteristics of a

natural person that allow or confirm the unique identification of said person,

such as facial images or fingerprint data;

Given the growing interest in using these systems in different fields and, as they are

of novel and very intrusive identification systems for the rights and

fundamental freedoms of natural persons, the constant concern of this

control authority has been shared by the rest of the authorities for years,

as evidenced by the Working Document on Biometrics, adopted on

08/1/2003 by the Group of 29, or the subsequent Opinion 3/2012, on the evolution of

biometric technologies, adopted on 04/27/2012, and which has led to the very

Community legislator includes this data among the special categories of data in

the GDPR.

Article 9.1 of the RGPD indicates:

“Treatment of special categories of personal data”

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."

In this way, its treatment being prohibited in general, any

exception to said prohibition shall be subject to a restrictive interpretation.

Biometric data have the peculiarity of being produced by the user himself.

body and definitively characterize it. Therefore, they are unique, permanent in the

time and the person cannot be released from it, they cannot be changed in case of

compromise-loss or intrusion into the system etc. Unlike a password, in

case of loss they cannot be exchanged. On the other hand, there are also risks

obvious if the technology used does not sufficiently guarantee that the template

obtained from the biometric data will not coincide with that used in other

similar systems. It is undeniable that the use of systems based on

biometric recognition can have advantages, such as registration of working hours, now

Well, it doesn't seem like it's the only system that can guarantee it. will have to

question whether the treatment is necessary in relation to the purpose pursued and the

objective proportionality of treatment. These elements must be studied together with

the informative principles of the regulations that concern us, in order to determine

if the measures implemented are proportional to the intrusion into the private sphere of

the interested parties they suppose.

The centralization of data stored on servers increases the risk of appropriation

improper use of data, as well as the seriousness of the consequences of a potential

system failure. Added to this are the products offered by developers and di-

signers of products related to biometric data, such as software and

Verification of its adaptation to existing security standards or those that may arise.

turn

According to the information provided by the claimed person, when entering the fingerprint,

“a number with many digits” has been generated by the hash function (application

of an algorithm) that provides a single value. What it means is that the information

collected biometric information, in this case, the image of a fingerprint, is processed

following procedures defined in standards and the result of that process is

stores in data records called signatures, patterns or "templates". These pa-

trons numerically record the physical characteristics that allow us to differentiate

you sound In the terminal or card machine, the offered pattern is compared when it is entered

the finger with the stored one, in order to record the day. It is estimated that the

The comparison does not take place one against one, that of the employee who agrees with his, but

with all those that are stored, performing a one-to-one comparison function.

several each time you enter or exit. In this case, even if not entirely saved

the image of the fingerprint, but a few digits, each of them in the form of a template, is

capable of uniquely identifying each employee by confronting the terminal with the

taking the footprint with the rest of the existing ones. The functions contained in

algorithm allow to extract the characteristic points of the footprint for later

comparison with a database associated with the set of users previously

stored, being able to identify its holder among all the templates,

processing personal data based on the processing of the fingerprint,

uniquely identifying that person.

It remains thus, accredited that the claimed person treats personal data of a biometric nature

of its employees, in this case for the purpose of time recording.

III

Of the initial prohibition of the processing of biometric data and its exceptionality are shown in recitals 51 and 52 of the RGPD, indicating: "Such personal data must not be processed, unless its processing is permitted in specific situations covered by this Regulation, taking into account Member States may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation to the fulfillment of a legal obligation or the fulfillment of a mission carried out in the public interest or in the exercise of public powers vested in the responsible for the treatment. In addition to the specific requirements of that treatment, the general principles and other rules of this Regulation should apply, especially in what refers to the conditions of legality of the treatment. Should be explicitly establish exceptions to the general prohibition of treatment of those special categories of personal data, among other things when the 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 freedoms. (52) “Likewise, exceptions must be authorized to the prohibition of processing special categories of personal data when established the Law of the Union or of the Member States and provided that the guarantees

appropriate, in order to protect personal data and other fundamental rights,

when it is in the public interest, in particular the processing of personal data in the

field of labor law, social protection law, including

pensions and for purposes of security, supervision and health alert, prevention or

control of communicable diseases and other serious threats to health. (...)"

The RGPD prescribes the exceptions to the treatment of biometric data in your

article 9.2, by indicating:

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

following:

a) the interested party gave their explicit consent for the processing of said data

for one or more of the specified purposes, except when the Right of

the Union or the Member States establishes that the prohibition referred to in the

section 1 cannot be lifted by the interested party;

"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 that it is so

authorized by the law of the Union or of the Member States or a collective agreement

in accordance with the law of the Member States establishing adequate guarantees

of the respect of the fundamental rights and the interests of the interested party;"

(…)

4. Member States may maintain or introduce additional conditions,

including limitations, with respect to the processing of genetic data, data

biometric or health-related data."

The LOPDGDD refers to these special category data in its article 9:

"1. For the purposes of article 9.2.a) of Regulation (EU) 2016/679, in order to avoid discriminatory situations, the consent of the affected party alone will not suffice to lift the ban on the processing of data whose main purpose is to identify your ideology, union affiliation, religion, sexual orientation, beliefs or racial origin or ethnic.

The provisions of the preceding paragraph will not prevent the processing of said data by protection of the remaining assumptions contemplated in article 9.2 of the Regulation (EU) 2016/679, when appropriate."

The obligation to record the daily working hours of employees does not come from contract, but of a law, the Workers' Statute, although its treatment through fingerprint registration should be necessary in order to fulfill said obligation, only, "to the extent" authorized by the law, either of the Union, or of the Member States, or a collective agreement, also within the framework of the right of the State, containing adequate guarantees regarding fundamental rights and of the interest of the interested party.

The correlation to this mention is found in article 9 of the LOPDGDD, which states:

In this sense, article 88 of the RGPD has established that the Member States may, through legislative provisions or collective agreements, establish more specific rules to ensure the protection of rights and freedoms in relation to the processing of personal data of workers in the la-labor, in particular, among others, for the purposes of complying with the obligations that are established by law or by collective agreement, the management, planning and organization of the worked. These rules must include adequate and specific measures to preserve

the human dignity of the interested parties, as well as their legitimate interests and their rights.
fundamental facts, in particular, in relation to, among others, the systems of super-
vision in the workplace.

IV

The limitation of the fundamental right to the protection of personal data must be the
strictly necessary. This implies that if the achievement of the intended purposes
can be done without processing personal data, this route will be preferable and
It will mean that it is not necessary to carry out any data processing. valued that
the collection, storage and use of data is necessary, which constitutes per se a
limitation of the right to data protection, must also comply with the regulations
in question. This therefore requires, first of all, to analyze and ensure that the collection of
data is necessary for the established or intended purpose and if it were, that it be
proportional.

Necessity is a fundamental principle when assessing the restriction of rights.
fundamental rights, such as the right to personal data protection. About him
principle of the need to process personal data, it can be said that
any data processing implies per se and from the beginning, the restriction of the fundamental right
on the occurrence of the collection and disposition of the same by the

know that you will operate with it. According to jurisprudence, due to the role that the treat-
processing of personal data performs for a series of fundamental rights, the
limitation of the fundamental right to the protection of personal data must be strict

strictly necessary.

Before implementing a fingerprint identity recognition system

fingerprint, the person in charge must assess if there is another less intrusive system with which

the same purpose is achieved. Section 72 of Guidelines 3/2019 on the

processing of personal data through video devices, of January 29,

2020, of the European Committee for Data Protection: “The use of biometric data and, in

particular, of facial recognition carry high risks for the rights of

the interested. It is essential that the use of such technologies takes place

duly respecting the principles of legality, necessity, proportionality and

minimization of data as established by the RGPD. Although the use of these

technologies may be perceived as particularly effective, those responsible for

processing must first assess the impact on the rights and freedoms

and consider less intrusive means of achieving its legitimate end of the

treatment. “

Opinion 3/2012, on the evolution of biometric technologies of 04/27/2012,

of the Article 29 Working Party (set up under Article 29 of Directive

95/46/EC, European independent advisory body on data protection

and right to privacy. Its tasks are described in article 30 of the Directive

95/46/CE and in article 15 of Directive 2002/58/CE), indicates that: “When analyzing the

proportionality of a proposed biometric system, it is necessary to consider

previously if the system is necessary to respond to the identified need, it is

that is, if it is essential to satisfy that need, and not just the most suitable or

profitable. A second factor that must be taken into account is the probability that the

system is effective in responding to the need in question in light of the

specific characteristics of the biometric technology to be used. a third

aspect to ponder is whether the resulting loss of privacy is proportional to the

expected benefits. If the benefit is relatively minor, such as a higher

comfort or a slight saving, then the loss of privacy is not appropriate. The

fourth aspect to assess the adequacy of a biometric system is to consider whether

a less invasive means of intimacy would achieve the desired end".

These assessments require exhaustiveness, starting in this case, not only from the

prohibition of treatment of these data, since we are faced with categories

of personal data, but the risks of using intrusive technology, the

biases or the likelihood of misidentification, identity theft

and the type of unique, permanent and invariable identity that the trace contains, its

impact on the privacy of individuals, security measures, the need and

proportionality or the aforementioned treatment.

Regarding proportionality, the Constitutional Court has indicated in the

Judgment 207/1996 that it is "a common and constant requirement for the

constitutionality of any restrictive measure of fundamental rights, among

them those that suppose an interference in the rights to the physical integrity and the

privacy, and more particularly of the restrictive measures of fundamental rights

adopted in the course of criminal proceedings is determined by the strict

observance of the principle of proportionality."

In this sense, we have highlighted that, in order to verify whether a restrictive measure of

a fundamental right surpasses the judgment of proportionality, it is necessary to ascertain whether

meets the following three requirements or conditions: "if such a measure is capable of

achieve the proposed objective (judgment of suitability); if, in addition, it is necessary, in the sense that there is no other more moderate measure to achieve such purpose with equal efficacy (judgment of necessity); and, finally, if it is weighted or balanced, because more benefits or advantages are derived from it for the general interest that harms other goods or values in conflict (judgment of proportionality in the strict sense).

In this way, if said purpose could be achieved by carrying out a activity other than the aforementioned treatment, without said purpose being altered or harmed, the latter activity should be chosen, given that the treatment of personal data implies, as established by our Court Constitutional, in Judgment 292/2000, of 11/30, a limitation of the right of person to have the information related to it."

In this sense, the analysis carried out by the working group created by article 29 of Directive 95/46/EC, in the Working Document on biometry, dated 08/01/2003, in which the following is stated:

"In accordance with article 6 of Directive 95/46/EC, personal data will be collected for specific, explicit and legitimate purposes, and will not be processed subsequently in a manner incompatible with said purposes. Furthermore, the data personal information will be adequate, pertinent and not excessive in relation to the purposes for those that are collected and for those that are subsequently treated (principle of purposes).

Compliance with this principle implies, first of all, a clear determination of the purposes for which the biometric data is collected and processed.

On the other hand, it is necessary to evaluate compliance with proportionality and legitimacy, taking into account the risks for the protection of the rights and fundamental freedoms of individuals and especially if the goals pursued they may or may not be reached in a less intrusive way.

Proportionality has been the main criterion in almost all decisions taken

until now by the authorities in charge of data protection on the

biometric data processing....

The use of biometrics also raises the issue of the proportionality of each

category of data in light of the purposes for which said data is processed. The data

biometrics can only be used in an appropriate, relevant and not excessive way, which

which supposes a strict assessment of the necessity and proportionality of the data

treated. For example, the French CNIL has rejected the use of fingerprints in the

case of children's access to a school cafeteria19, but has accepted with the same

order the use of the results of samples of the hands. The Portuguese authority

data protection has recently made an unfavorable decision on the

use of a biometric system (fingerprints) by a university

to control the attendance and punctuality of non-teaching staff"

In the present case, it should have been taken into account initially, not only

as part of the data protection impact assessment, but as a rule

general in any treatment an examination on:

-suitability: "if such a measure is capable of achieving the proposed objective". In this

case, the defendant progressively establishes the system, despite the warning of the

claimant on the legitimate basis of the consent of the employees, to which

then reference will be made, collecting the consent document from everyone. The

limitation of the rights of all employees is against the fulfillment of a

labor legal obligation to record the daily shift, although the means for this that
they can be varied, they do not have to suppose the interference in the rights of the
employees as it happens here. It is necessary to apply, case by case, the principle of
suitability with respect to the ends pursued, which implies a kind of
Data minimization obligation by the data controller.
-The need for treatment is an essential requirement that any me-
proposed measure involving the processing of personal data. It will be justified on
basis of objective evidence and is the first step before assessing the proportionality of
the limitation. Necessity is also fundamental when assessing the legality of the
treatment of personal data. The processing operations, the categories of
processed data and the duration of data conservation will be necessary for the
purpose of treatment.
Proof of need for treatment for any exercise limitation
rights to the protection of personal data must be strict, and the data must be treated
themselves only in strictly necessary cases, since in principle, any
data processing operation limits the right to data protection
regardless of whether such limitation may be justified. Is
Necessity as suitability for the purpose of the treatment must be justified in the
documentation of compliance that the person in charge must have in accordance with the
article 5.2. of the RGPD, and may also be contained in the evaluation document
data protection impact if the elements to be carried out concur.

The need must relate to whether personal data is processed on the basis of a
objective evidence, according to the purposes to be determined, if those
personal data or if the purpose can be fulfilled without processing that personal data.
Necessity implies that a combined evaluation, based on facts, is required.
on the effectiveness of the measure for the objective pursued and on whether it is less in-

trusive compared to other options to achieve the same goal. In this

case it is about data processing through the registration of fingerprints for compliance

ment of the legal obligation imposed on the employer of the registration of working hours

each worker in article 34.9 of the Workers' Statute, a rule that

does not anticipate that biometric data will be used for this. The desired ends are the registration

of the data, however the claimant does not pay for the need to implement the registry

of the fingerprint for said purpose or that it is essential, indicating the reasons that

its non-use prevents obtaining that purpose. If the draft measure does not pass the necessity test,

cesity, it is not necessary to examine its proportionality.

Need should not be confused with system utility. It may be easy to not

having to carry a card, it's automatic and instant. Obviously a system

fingerprint recognition can be useful, but it does not have to be objectively

necessary (the latter being what really must be present). as set

WG29 - Opinion 3/2012 on the evolution of biometric technologies - should

be examined “if it is essential to satisfy that need, and not just the most suitable

or profitable.

In this sense, the AEPD, analyzing the need for a treatment, concludes that, “If

is necessary or not, in the sense that there is no other more moderate measure for the

achievement of such purpose with equal efficiency because it can be carried out manually

activity. The term need should not be confused with useful but if the treatment is

objectively necessary for the purpose” -by all, PS/00052/2020-.

The need is also a principle of data quality and a recurring condition

in almost all the requirements on the legality of the processing of personal data

derived from the right to Data Protection. If there is no objective need for

treatment, if it is not essential to satisfy that need, the treatment is not

proportional or lawful.

-Proportionality, Proportionality is a general principle of EU law.

It restricts the authorities in the exercise of their powers by requiring them to achieve a

balance between the means used and the intended objective. In the context of rights

fundamental rights, such as the right to the protection of personal data, the proportion

tionality is key to any limitation of these rights.

Proportionality requires a logical link between the measure and the objective pursued.

Furthermore, for a measure to comply with the principle of proportionality, the advantages

resulting from the measure should not be compensated for the disadvantages caused by the

measure with respect to the exercise of fundamental rights. In other words, the

limitation of the right must be justified. The safeguards that accompany a

measure can support the justification for a measure. A precondition is that

the measure is adequate to achieve the intended objective. In addition, when evaluating the treatment

processing of personal data, proportionality requires that they are only collected and

cease those personal data that are adequate and relevant for the purposes of the

prosecution.

The proportionality judgment leads to the adoption of the system, considering that

necessary, produce less interference in the law, so that it does not

there could be an equally effective system whose implementation would imply less

interference in the right of the employees, that is to say, the

proportionality in its specific context, proving that technical measures

less intrusive do not exist or would not work.

And it is at this point that everything that has been

been indicating in relation to the special nature that biometric data

conferred by the RGPD and that requires special attention not only to proportionality but

to the data minimization itself; that is, that the data is only processed

as long as it is completely essential for the fulfillment of the

purpose pursued.

If the three requirements indicated are not met, it can be stated that the need

to go for the time control to take the fingerprint of the employees is not

essential, as there are other means that are suitable for this purpose. The system

nor would it comply with the requirements of proportionality and suitability. The truth is

In this case, no documented analysis of these elements was provided,

which, as indicated, would form an essential part of the aforementioned impact assessment,

the infraction of which is considered to have been committed.

On the other hand, the European Data Protection Supervisor has issued, among others, the

10/7/2020, a note on the current state of biometrics, which can be consulted

in

https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/

state-biometrics-wojciech-wiewiorowski_en.

v

In this case, the respondent indicates that the legitimizing basis of the treatment, based on

of those established in article 6.1 of the RGPD, it would be that of express consent.

He adds that there are two others, compliance with a legal obligation, 6.1.c) of the
RGPD and maintenance of compliance with the contractual relationship, 6.1 b), although the
obligation does not derive from the contract but from a norm. So, for example, in the context
labor, derives from the contract the treatment of the information on the salary and the data
of the bank account so that the salary can be paid, so that there is a link
direct and objective link between the processing of the data and the purpose of the execution of the
contract. The registration of the fingerprint for compliance with the registration obligation
other day as proposed by the respondent, if the prerequisites are met,
It is necessary for the execution of the contract, otherwise it would be necessary for the fulfillment of the contract.
compliance with a legal obligation that must be adapted to the general principles of
processing of data, after overcoming the prohibition of treatment for the reasons
assessed in article 9 of the RGPD
Notwithstanding what has been said, consent within an employment relationship is a
exceptional legitimizer for:
-The very definition of consent, "any manifestation of free will, specifically
fica, informed and unequivocal by which the interested party accepts, either through a de-
declaration or a clear affirmative action, the treatment of personal data that con-
looming" does not start from a position of balance in the relationship. as you have underlined
WG29 in various opinions, consent can only be valid if the interested party
can really choose and there is no risk of deception, intimidation, coercion or con-
significant negative consequences (for example, substantial additional costs) if not
you give your consent. Consent will not be free in those cases in which
there is an element of compulsion, pressure or inability to exercise free will.
-The fact that it can be withdrawn whenever the owner wishes, an element that must be
include in the clause before it is provided, provided that the withdrawal of consent
The process will not entail any cost for the interested party and, therefore, no disadvantage

for those who withdraw consent.

-There should be the possibility of not granting the same, and therefore offer alternatives.

-Articles 16 to 20 of the RGPD indicate that (when the data processing is based

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

in the consent) the interested parties have the right to the deletion of the data when

where consent has been withdrawn.

SAW

The defendant was charged with processing personal data of a special category

and there is an obligation to have an Impact Assessment on Protection

tion of Personal Data (EIPD) breached article 35 of the RGPD:

"1. When a type of treatment, particularly if it uses newer

technologies, due to their nature, scope, context or purposes, entails a high risk for

the rights and freedoms of natural persons, the person responsible for the treatment carried out

will carry out, before treatment, an evaluation of the impact of treatment operations.

ment in the protection of personal data. A single evaluation may address a

series of similar processing operations involving similar high risks.

2. The data controller shall seek the advice of the protection delegate

data, if appointed, when conducting the impact assessment relating to the

Data Protection.

3. The impact assessment related to data protection referred to in the

paragraph 1 will be required in particular in case of:

a) systematic and exhaustive evaluation of personal aspects of natural persons

that is based on automated processing, such as profiling, and on

whose basis decisions are made that produce legal effects for natural persons.

cases or that significantly affect them in a similar way;

b) large-scale processing of the special categories of data referred to

Article 9, paragraph 1, or personal data relating to convictions and offenses

penalties referred to in article 10, or

c) large-scale systematic observation of a publicly accessible area.

4. The control authority will establish and publish a list of the types of operations

processing purposes that require an impact assessment relating to the protection

of data in accordance with section 1. The control authority shall communicate these

lists to the Committee referred to in article 68.

5. The control authority may also establish and publish the list of types

of treatment that do not require impact assessments related to the protection of

data. The control authority shall communicate these lists to the Committee.

6. Before adopting the lists referred to in paragraphs 4 and 5, the authority of

competent control will apply the coherence mechanism contemplated in article

63 if those lists include treatment activities that are related to the offer

of goods or services to interested parties or with the observation of the behavior of these

in several Member States, or processing activities that may substantially affect

especially to the free movement of personal data in the Union.

7. The evaluation must include at least:

a) a systematic description of the planned treatment operations and the

purposes of the treatment, including, where appropriate, the legitimate interest pursued by the

data controller;

b) an assessment of the necessity and proportionality of the treatment operations

lie with respect to its purpose;

c) an assessment of the risks to the rights and freedoms of data subjects to

referred to in section 1, and

d) the measures envisaged to deal with the risks, including guarantees, security measures,

security and mechanisms that guarantee the protection of personal data, and to

show compliance with this Regulation, taking into account the rights

and legitimate interests of the interested parties and other affected persons.

8. Compliance with the approved codes of conduct referred to in article

40 by those responsible or in charge, it will be duly taken into account

account when assessing the repercussions of processing operations carried out by

said managers or managers, in particular for the purposes of impact assessment

regarding data protection.

9. When appropriate, the person in charge will obtain the opinion of the interested parties or their

representatives in relation to the planned treatment, without prejudice to the protection of

public or commercial interests or the security of processing operations.

10. When the treatment in accordance with article 6, paragraph 1, letters c) or

e), has its legal basis in Union Law or in the Law of the Member State.

law that applies to the person responsible for the treatment, such Law regulates the operation

specific treatment or set of operations in question, and has already been carried out

a data protection impact assessment as part of an assessment

general impact in the context of the adoption of said legal basis, the apart-

Items 1 to 7 shall not apply except if the Member States deem it necessary

It is advisable to proceed to said evaluation prior to treatment activities.

11. If necessary, the person in charge will examine whether the treatment is in accordance with

the impact assessment related to data protection, at least when there is a

change in risk represented by treatment operations."

In development of paragraph 4, the Director of the AEPD published an indicative list of

after processing that require an impact assessment relating to the protection of

data, indicating: "At the time of analyzing data processing, it will be necessary to

perform DPIA in most cases where such treatment complies with

two or more criteria from the list below, unless the treatment is in-

is on the list of treatments that do not require EIPD referred to in article

35.5 of the RGPD." "The list is based on the criteria established by the Working Group

under Article 29 in guide WP248 "Guidelines on impact assessment related to

protection of data (EIPD) and to determine if the treatment "entails pro-

probably a high risk" for the purposes of the RGPD", complements them and must be understood

as a non-exhaustive list:

"4. Treatments that imply the use of special categories of data to which

referred to in article 9.1 of the RGPD, data related to convictions or criminal offenses

data referred to in article 10 of the RGPD or data that allow determining the

financial situation or equity solvency or deduce information about the people

nas related to special categories of data.

5. Processing that involves the use of biometric data for the purpose of

uniquely identify a natural person.

9. Data processing of vulnerable subjects…”

At the same time, the Guidelines on impact assessment relating to the

Data Protection and to determine whether the processing is likely to entail a high

risk for the purposes of the RGPD adopted by the working group 29, on April 4, 2017,

points out:

“In order to offer a more specific set of treatment operations that re-

want DPIA due to its inherent high risk, taking into account the elements

particulars of article 35, paragraph 1, and article 35, paragraph 3, letters a) to c), the

list to be adopted at national level under Article 35(4) and the

Recitals 71, 75 and 91, and other GDPR references to processing operations

that are “likely to pose a high risk”, all nine criteria should be considered

following:

“7. Data relating to vulnerable data subjects (recital 75): The treatment of this

type of data represents a criterion due to the increased imbalance of power between

the interested parties and the data controller, which implies that people can

They are unable to authorize or deny the processing of their data, or to exercise their rights.

Rights. Vulnerable data subjects may include children (considered to be

are not capable of denying or knowingly and responsibly authorizing the treatment

of your data), employees”

The purpose of the impact assessment, within the process of regulatory compliance

vo “accountability”, supposes the taking of own responsibility for what is done with

personal data and how it complies with the principles, incorporating appropriate

measures and records to be able to demonstrate compliance. The organizations

must demonstrate that they are complying with the norm, including measures of

documentation on how the data is processed, for what purpose, until when, and

document treatments and procedures to focus the issue from a

early stage of construction of the treatment system. Its implantation

enables the minimization of risks at the time of processing the data, taking into account

ta as required in the impact assessment, necessity and proportionality

of them, the amount of data, etc. Within the EIPD, the initial right would appear

data and scope of the data holders and assessing the risks, if any

guarantees, analysis of how they are affected... so that before proceeding with the treatment

there is a document available that supports subsequent management, helping to identify

tify and minimize the risks of a data processing project that will result

or affect in this case in a high degree of risk to individuals, employees of the re-

claimed, given the specific form of treatment the nature of the context and the pro-

deposits.

The implementation of the time registration system without carrying out the mandatory EIPD that

responded in the specific case in accordance with all of the foregoing, given the

high risk that processing poses to the rights and freedoms of employees

two, it constitutes a clear breach of the GDPR.

As for the security measures provided by the respondent, his own, which appear

ran in document 5.4 it should be indicated that they are only the general framework of actions

regarding the management of information systems and the general criteria that are

They must be specified for each type of treatment that is carried out. It is credited not

stating any reference other than to the treatment of video surveillance, and having

implanted the biometric treatment as of October 2019, the document does not include

any assessment of the type of data, the need, proportionality, etc., aspects

documents to be finalized.

Regarding the measures that could have an impact on the risks collected,

in the treatment order contract, in its ANNEX III, data security, re-

fers the security of the data that is stored, on which it is not deepened.

It only indicates that action procedures related to safety will be implemented.

technical and organizational authority of data processing and maintenance of secrecy

professionals used with VisualTime SaaS, which guarantee confidentiality, integration

ity and availability of the same, storage in the cloud, as well as the re-

terminological references that are usually implemented literally about measures of

security that the processing order must comply with.

The EIPD is a necessary step for data processing, not being the only one required.

ble, it is a budget to which must be added the rest of the legal requirements for the

processing, legitimating basis and respect for the fundamental principles of processing

Data protection provided for in article 5 of the RGPD.

From the documentation in the file and as inferred from the actual facts

there is no evidence of carrying out the protection impact assessment.

data tion.

7th

The RGPD determines in article 83.4 a): "Infringements of the following provisions

The following will be sanctioned, in accordance with section 2, with administrative fines of

EUR 10,000,000 maximum or, in the case of a company, an equivalent amount.

2% maximum of the total global annual turnover of the fiscal year

previous financial statement, opting for the highest amount:

the obligations of the person in charge and the person in charge in accordance with articles 8, 11,

25 to 39, 42 and 43;”

The LOPDGDD establishes in its article 73.t):

“Based on the provisions of article 83.4 of Regulation (EU) 2016/679

are considered serious and will prescribe after two years the infractions that suppose a

substantial violation of the articles mentioned therein and, in particular, the following

following:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

23/25

t) The processing of personal data without having carried out the evaluation of the

impact of processing operations on the protection of personal data in

assumptions in which it is required.”

viii

Article 58.2 of the RGPD provides the following: "Each control authority will have

of all the following corrective powers indicated below:

b) send a warning to any person responsible or in charge of the treatment

when the treatment operations have violated the provisions of this

Regulation

d) order the person in charge or in charge of the treatment that the operations of

treatment comply with the provisions of this Regulation, where appropriate,

in a certain way and within a specified period;

i) impose an administrative fine pursuant to article 83, in addition to or instead of

gar of the measures mentioned in this section, according to the circumstances of

each particular case;”

Indicates article 77 of the LOPDGDD:

"1. The regime established in this article will be applicable to the treatment of

those who are responsible or in charge:

…j) The consortiums.

2. When those responsible or in charge listed in section 1 committed

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

organic, the data protection authority that is competent will dictate

resolution sanctioning them with a warning. The resolution will establish

also the measures that should be adopted to stop the behavior or correct it.

the effects of the infraction that had been committed.

The resolution will be notified to the person in charge or in charge of the treatment, to the body of the

that depends hierarchically, where appropriate, and to those affected who had the condition

interested party, if any.

3. Without prejudice to what is established in the previous section, the protection authority

of data will also propose the initiation of disciplinary actions when there are

sufficient evidence for it. In this case, the procedure and the sanctions to be applied

will be those established in the legislation on disciplinary or sanctioning regime that

result of application.

Likewise, when the infractions are attributable to authorities and managers, and

proves the existence of technical reports or recommendations for the treatment that

had not been duly attended to, in the resolution imposing the

The sanction will include a reprimand with the name of the responsible position and

will order the publication in the Official State or Autonomous Gazette that

correspond.

4. The data protection authority must be notified of the resolutions that

fall in relation to the measures and actions referred to in the sections

previous.

5. They will be communicated to the Ombudsman or, where appropriate, to similar institutions

of the autonomous communities the actions carried out and the resolutions issued

under this article.

6. When the competent authority is the Spanish Agency for the Protection of

Data, it will publish on its website with due separation the resolutions

referred to the entities of section 1 of this article, with express indication of the

identity of the person in charge or in charge of the treatment that would have committed the

infringement.

When the competence corresponds to a regional authority for the protection of

data will be, in terms of the publicity of these resolutions, to what your

specific regulations."

Regarding the allegation of not imposing the sanction, once started, the process continues.

ex officio procedure, and it is appreciated that the infraction was perfected at

time of the claim and the start of the agreement. The correction of the

infraction, in this case it can allow the non-imposition of corrective measures or

adequacy of the data processing in question, but does not allow the file of the

infraction as if the behavior analyzed had not existed.

Therefore, in accordance with the applicable legislation,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: SANCTION the CONSORTIUM FOR THE

CONSTRUCTION, EQUIPMENT AND OPERATION OF THE SPANISH HEADQUARTERS

FROM THE EUROPEAN NEUTRON SOURCE BY SPALATION, with NIF

G95455473, for a violation of article 35 of the RGPD, in accordance with the

article 83.4 a) of the RGPD, and for prescription purposes in article 73.t) of the

LOPDGDD.

SECOND: NOTIFY this resolution to the CONSORTIUM FOR THE

CONSTRUCTION, EQUIPMENT AND OPERATION OF THE SPANISH HEADQUARTERS

FROM THE EUROPEAN NEUTRON SOURCE BY SPALATION.

THIRD: COMMUNICATE this resolution to the OMBUDSMAN, of

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

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

counting 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 13/07, 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,

may provisionally suspend the firm resolution 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

LPCAP. You must also transfer to the Agency the documentation that accredits the

effective filing of the contentious-administrative appeal. If the Agency did not have

knowledge of the filing of the contentious-administrative appeal within the period of

two months from the day following the notification of this resolution, I would

The precautionary suspension has ended.

Sea Spain Marti

Director of the Spanish Data Protection Agency