 File No.: PS/00218/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

BACKGROUND

FIRST: CLAIMANT (appears in the GENERAL ANNEX) (hereinafter, the complaining party), dated 06/22/2020, files a claim with the AEPD. The claim is directed against EUROVILLAS CONSERVATION COLLABORATING URBAN DEVELOPMENT ENTITY, with NIF G79414033, at calle ***DIRIMIENTO.1, Madrid (hereinafter, the claimed party). The motives on which the claim is based are that the respondent established a daily registration system for employees' workday through facial recognition (RF) technique.

Manifests:

-On 02/13/2020, the respondent installed a time registration system in the workplace “by fingerprint”, modifying the prior use of the card. The representation of employees sent a letter on 02/17/2020, of which a copy is attached as DOCUMENT 1, signed by the claimant and two other employees, as "Delegates XXXXXXXXXX", in the that mention that compliance with article 9.2.b) of the 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 the processing of personal data and the free circulation of these data (hereinafter GDPR); and that the measure has been taken without having communicated or negotiated with the workers' representatives, requesting that they switch to other systems.

-On 02/17/2020, the respondent handed in a communication from the system implanted "tactile recognition", with start-up indication on 03/01/2020.

-In a letter from the respondent on the same date, 02/17/2020, he replied to the claimant's

17/02 indicating that "there is no obligation to obtain consent since the system

system implemented pursues legitimate interests on the part of the company", "given that

the labor legislation obliges to record the number of hours that the workers perform

yes", and

that "the use of the cards that had been used caused fraud in the management and therefore

They were not adequate means to the end pursued. Accompany DOCUMENT 3 with the

received, which verifies these claims.

-The claimant wrote to the respondent on 03/11/2020, requesting:

"Characteristics of the treatment, form of storage and responsible for the custody,

way in which the records of working hours will be available, both for workers and

for their representatives.

Accompanying DOCUMENT 4 containing the response of 03/12/2020, indicating that the

Responsible for the data is the person appointed by the company to process the data of the users.

workers and that due to the situation created by the "coronavirus", the

change the current time registration system, "for one of facial vectors, in which case,

would store a photograph, just like the system used with cards

previous".

-The claimant states that on 04/30/2020, the respondent communicates a change in the

system of time records originated by the COVID-19 disease and that will be implemented at

as of 05/06/2020. It consists of the identification of the personnel by data of their own face,

"through facial vectorization" "This system works from the identification of a

percentage of features extracted from the face, without taking a three-dimensional image

of the faces “we understand that this measure is less invasive than the recording of the moment

of signing by camera, which also involved physical contact with a card reader

shared. The sole purpose of this data is the signing of personnel and analysis of the times of

work for compliance with decree law 8/2019, in order to analyze the data in taking

of decisions and the defense of their legitimate interests. These data will be found in the

servers of this entity, in no case in the cloud”. Accompanies DOCUMENT 6.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5/12, of

Protection of Personal Data and guarantee of digital rights (hereinafter

LOPDGDD), on 07/7/2020, said claim was transferred to the claimed party, to

to proceed to its analysis and inform this Agency within a month of:

“1. The decision adopted regarding this claim.

2. Report on the causes that gave rise to the incident that gave rise to the claim.

3. Risk Analysis and Impact Assessment Study related to data processing

personal object of the claim.

4. Base of legitimacy of said treatment and justification.

5. Report on the measures adopted to prevent similar incidents from occurring,

dates of implementation and controls carried out to verify its effectiveness.

6. Any other that you consider relevant.”

On 08/05/2020, this Agency received a written response indicating:

1) It is an "administrative entity" "dependent on" the Community of Madrid, although with

its own legal personality and full capacity for autonomy to fulfill its

purposes, in accordance with the law and the Bylaws, and which basically consist of the

conservation of free spaces of public domain and use, and in its case of private ones, and

the maintenance of the endowments such as facilities and infrastructures of the urbanization.

The nature of "administrative entity" is expressly included in article 26.1 of the Royal

Decree 3288/1978, of 08/25, which approves the Urban Management Regulation

for the development and application of the Law on Land Regime and Urban Planning

(RGU) “the collaborating urban entities will have an administrative and

They will depend in this order on the acting urban administration”.

Provides a copy of its Statutes, the current version of which is published in the BOCM of

05/29/2014. The following provisions are considered important for the case:

“Art 1- A collaborating urban entity of an administrative nature is constituted with

own legal personality and full legal capacity from its registration in the registry of

collaborating urban entities of the Ministry competent in urban matters of

the Community of Madrid.”

This conservation entity was established on a mandatory basis by virtue of the

determinations of the special plan city of the Americas, today Euro Villas, approved

definitively on March 23, 1988 and will be composed of all the owners

included in its territorial scope.

The conservation entity shall be governed by the provisions of these statutes and in what is not

foreseen by them by articles 24 to 30 and 68 to 70 of the RGU of August 25, 1978 and

other concordant and complementary provisions.

“Article 3, object: This entity has as its object the conservation of the urbanized work, of

the free spaces of public domain and use and, where appropriate, of the private ones and the maintenance

of the endowments and installations of urban services and infrastructures in accordance with

the provisions of article 32 of these statutes.”

Article 4 indicates the purposes basically of execution of works necessary for the repair and maintenance whose conservation is necessary in terms of the use and utilization of the goods and services.

Article 5 establishes: "To the Ministry competent in urban matters as acting administration corresponds to the following functions: approve the text of the statutes for the constitution of the conservation entity, approve the constitution of the conservation entity for registration in the registry. In section c it is indicated that without prejudice to the fact that the acting administration is the Ministry of Public Works and Urbanism and Transportation, will correspond to the Municipalities in which the urbanization, the use of the enforcement procedure for the collection of amounts owed by any of the members of the Conservation Entity. In section d) it indicates that It corresponds to the acting administration to resolve the appeals against agreements of the entity, as well as agreeing the dissolution of the entity in the cases contemplated in the article 40 of the statutes and any other powers resulting from urban planning legislation and autonomous."

Article 19 establishes as powers and functions of the Governing Council, the appointment and separation of personnel and indication of their work regime and the administration of the entity.

2) The entity has its own equipment, machinery and personnel to undertake its tasks of conservation and maintenance of the infrastructures and the public domain of the organization. "It brings together some 4,000 owners of plots on which there are built around 3,000 single-family homes that are inhabited by a population greater than 10,000 inhabitants.

Currently, the staff is made up of 38 workers who provide their services in some cases on a shift basis, with emergency services that cover a attention 24 hours a day. The review of these personnel and the verification of their attendance

to the workplace has always been subject to control. “A few years ago he signed up”, then he

made use of individual cards, but when fraud was detected with the cards that were left to

other employees, "a file system was established" by means of fingerprints and

subsequently, due to the risks of COVID-19, the system was changed to RF.

3) “The registration of working hours is mandatory for the company by virtue of article

34.9 of the Workers' Statute”. “Given the right and at the same time the obligation that the

Entity to keep a control and record of the workers' day that is reliable, the

system implemented is effective and proportional, as well as the most appropriate to guarantee

the health of workers, in these times of pandemic.” “The basis of legitimacy for the

The treatment of these data is given by the existing employment contract with the users (art.

6.1.b GDPR); the legal obligation to carry out a record of the working hours of employees

employees of the Entity (art. 6.1.c) and the company's own need to control employees

workers (art. 6.1. f), so that the Entity itself can perform the functions of

public interest entrusted to it given its nature as a public administration (art. 6.

1.e).”

4) The systems used by the entity in no case keep images or photographs

of the fingerprint or face of the person, but they are biometric systems in which to

its operation do not use images of fingerprints or faces, but mere descriptions of

these that are translated into the takings of various minutiae or patterns of the drawing of the footprint of the

face. Therefore, the system only takes a few minutiae or special features

concrete, in general the position or dimensions, elements of the footprint or the face

fundamentally, that they do not allow to reconstruct from them the imprint or the face of a person, so they consider that they do not allow the unequivocal identification of the most than within a small group of people such as the entity's staff. "The system is installed on a separate, password-protected computer to which you only have access a person and that the statistical biometric data, are encrypted, are not removable, nor knowable, because they are part of the program itself, without being able to be used to no other purpose." You understand that you are acting at all times in accordance with the law.

THIRD: On 09/04/2020, the Director of the Spanish Agency for Data Protection agreed to admit the claim for processing.

FOURTH: The General Subdirectorate for Data Inspection proceeded to carry out preliminary investigative actions to clarify the facts in question, in under the investigative powers granted to the supervisory authorities in article 58.1 of the RGPD, in accordance with the provisions of Title VII, Chapter I, Section second, of the LOPDGDD, having knowledge of the following extremes:

It asked the respondent to provide the risk analysis, the impact assessment of the treatment of biometric data and system characteristics.

On 10/29/2020, it was answered that "this claim has already been answered in the within the procedure of transfer and admission of the claim."

FIFTH: On 09/02/2021, the Director of the AEPD agreed:

URBAN DEVELOPMENT ENTITY

"INITIATE PUNISHMENT PROCEDURE

EUROVILLAS CONSERVATION COLLABORATOR, with NIF G79414033, by the

alleged infringement:

-Of article 9.2.b) in relation to 6.1 of the RGPD, typified in article 83.5.a) of the RGPD

-From article 35 of the RGPD, typified in article 83.4.a) of the RGPD.”

(…)

“THAT for the purposes provided in art. 64.2 b) of Law 39/2015, of 1/10, of the Procedure

Common Administrative of Public Administrations (hereinafter, LPACAP), the

sanctions that could correspond would be fines of 100,000 euros, and 20 thousand euros,

as specified, without prejudice to what results from the instruction.”

SIXTH: On 09/17/2021, allegations are received in which the respondent states:

1- It is considered to be included in section d) of article 77.1 of the LOPDGDD as a

public entity and public law entity linked to or dependent on the administrations

public”, for which a sanction of warning would proceed in his case. Considers,

furthermore, that it does not matter whether or not the public entity is carrying out a public activity,

because the regulations regulate the possibility of sanctioning for what it is, an administration

public, and not by the activity that is carried out. The cited article states that the “

Public Administrations will be sanctioned with a warning for the mere fact of being,

and as long as they meet that condition, without the legal system establishing that this only

will happen when they perform public functions, which is an expansive interpretation, or more

well, an "ex novo" legal creation of that Agency, given that it lacks any legal support and

There is no norm that gives rise, even to that interpretation, without, on the other hand, the

infractions of which the Entity is accused can be considered as private law.”

It is immaterial whether the labor contracting of the entity's workers is of a

private. It indicates that it makes no sense to separate which spheres the activity can affect, given

the administrative raison d'être of the entity itself and its public functions that it performs. I do not know that

before an issue of a labor nature, but "when faced with a matter of data protection,

that must be fulfilled by the administrative entity in the exercise of its public activity and with the intervention of its operating governing bodies, whose activity is subject to administrative law."

Decisions related to dismissals, staff organization, and any matter employment, are adopted by the Governing Board, all these issues being subject to the administrative law, and may be challenged in appeal before the CCAA of Madrid or via contentious (art 38 of the Statutes). “The situation is similar to what happens with the claims of delinquent owners of the entity, in which the Supreme Court has said that it is only competent for its knowledge in the contentious jurisdiction-administrative”. For example, the decision of 05/30/2012, resource 203/2009. Notes that even when the employees sue the entity for employment, given the nature of public administration of the same, they do not have to carry out acts of prior conciliation indicated in articles 63 and 64 in relation to 69.1 of the law of social jurisdiction, which

which shows that it is not a private relationship that exists with said employees of the entity.

2- "The initiation of the sanctioning procedure is by the facial recognition system, implemented according to that Agency, since May 6, 2021. With this, it is being recognized the validity of the fingerprint recognition system that previously had implanted the Entity.” “It is therefore, the change of the system, of fingerprint recognition fingerprint to facial, which would generate the infractions that are attributed to the Entity.” Considers that if the fingerprint takes the minutiae, in the RF, it is done on the face, being in both cases

Likewise, they do not serve to uniquely identify a person. It is not about data
special character because no images or photographs of the face are preserved, which for its
operation use "mere descriptions of these", "patterns of drawing the face",
position or dimensions of elements that do not allow to reconstruct from them the face of
a person, "which could also coincide in many other people, so they do not
allow the unequivocal identification of the subject, rather than within a small group of
people, such as the entity's staff". Data stored on a computer is
only accessible to one person, being encrypted and encrypted. Consider that it would not be
application of the prohibition of article 9.1 of the RGPD because "biometric data is not previously
aimed at unequivocally identifying a natural person."
Therefore, not being data of a special nature, it is not mandatory to provide the Evaluation of
Impact established in article 35 of the RGPD.
3-The main cause and context that motivated the change of a time registration system for
fingerprint to one of RF, was due to the extraordinary and serious situation derived from the alert
due to the pandemic, "which endangers the health and even the lives of workers
of the Entity, and with it, that the Entity can fulfill its purposes and obligations." Tasks
carried out by its personnel affect public health-cleaning, wading streets,
maintenance of the sanitation network, lighting, etc., along with disinsection that
it affected 10,000 residents, who at that time were coming out of confinement. I know
he intended not to touch the fingerprint reader and put his finger on the sensor. consider proportional the
system as it is a reliable and effective system, and the most appropriate to guarantee the health of
the employees.
4- Considers that the basis of legitimacy of the treatment is given by
-"The employment contract with users, art 6.1.b) of the RGPD
- The legal obligation to carry out a record of the working hours of employees.
employees of the entity, art 6.1.c) of the RGPD

-the very need of the company to control the workers (art. 6.1. f), of

so that the Entity itself can perform the functions of public interest that it has

entrusted, given its character of public administration (art. 6. 1.e).”

5- “With the improvement of the epidemiological situation, we have returned to the card transfer system,

Although negotiations are under way."

6- In the agreement, it is analyzed as the only possibility of legality of the treatment, the labor,

contemplated in letter 2.b) of article 9 of the RGPD, concluding that it does not proceed for three

issues:

a) It is said that it is not justified that the treatment through RF is necessary for the

compliance with labor obligations such as the registration of working hours and this

because that control had already been carried out previously with the card system. Considers

said system change was necessary because the cards were lent by some employees to

others.

b) Letters g) and h) of article 9.2 of the RGPD, by themselves, individually, and more

in relation to each other, with letter b), would justify special treatment, given the

extraordinary pandemic situation that we have experienced and that has been exposed. the letter g)

enables in the event that it is "necessary for purposes of essential public interest", being

prevent the spread of COVID an essential public interest, with recommendations for

there was no interpersonal contact or contact with surfaces. Also note that the letter

h) better enables the treatment, "it is necessary for purposes of preventive or occupational medicine",

being that the purpose that has moved the change of the system of hour records, to avoid the

infections among the entity's workforce.

7- It is said that the negotiation or consultation with the staff representatives was not respected,

but this was not the case, as it was reported, negotiated and finally maintenance was chosen

of facial registration while the pandemic lasted, and it should also be noted that "the

representatives of the workers never wanted to make a claim before the

AEPD, but simply make a query".

8- The defendant is an entity that provides public service, non-profit. acted with

encouragement to protect the health of its staff, in order to ensure that it could provide its

service that qualifies as essential during confinement, among a staff, which was affected

high spread of the disease. For all these reasons, he considers that he cannot

consider the defendant guilty. It adds, that in addition the sanction is disproportionate, for:

a) in the infringement of article 9.2.b) in relation to 6.1 of the RGPD, considers that

can produce the aggravating:

- of 83.2.a) of the RGPD, since the infringement is already of a very serious nature, "it cannot be used

that same intrinsic gravity in the infringement itself to add an aggravating circumstance to it"

"You are being sanctioned twice for the same conduct."

-from 83.2. b) of the RGPD for the same reason, the negligence is already incorporated in the type that is

sanctions, assuming a fictitious sum of aggravations that is not appropriate.

-of article 76.2.b) of the LOPDGDD, does not consider it relevant, since it is not an entity with

great experience in data processing with these special characteristics.

-of article 83.2.k) of the RGPD, being again an aggravating circumstance already included in the sanction as

very serious, not contemplating the cause that is manifested as an aggravating circumstance in the aforementioned article

b) In the violation of article 35 of the RGPD, some of the issues that are indicated as

aggravating circumstances of the infraction, would already be incorporated in this same infraction, again

they are being punished twice, so it would be the same conduct or sanctioning reproach and

Specifically, it considers that the aggravating factors cannot be caused by:

-article 83.2.b) by a qualified degree of degree of diligence, as it does not contemplate any type

of analysis on the treatment, which is maintained during the processing of the transfer,

continuing to carry out the treatment (93.2.1 of the RGPD). "If what is punished is not

have carried out an impact assessment, because it is considered that before implementing a

facial recognition system, that this must be done, cannot be considered aggravating

not having done the analysis or the evaluation itself".

Considers should be assessed, as mitigating factors:

- The situation of serious national health emergency and exceptionality (with states of

alarm) derived from the pandemic experienced. It cannot be ignored that we are talking about the month

May 2020, full state of alarm with home confinement situation. The

ultimate claim and that motivates the change of system to RF was the fight against the pandemic and

guarantee or at least reduce the chances of contagion of the workforce.

He considers that the sanctions are not even in due proportion to each other:

They propose 100,000.00 euros and 20,000.00 euros. Article 83.5.a) of the RGPD, applicable

to the first infringement, refers to 4% of the turnover in the case of companies and

with a maximum possible total of 20 million euros, while in 83.4 of the RGPD

applicable to serious sanctions, this percentage is reduced to 2% with a maximum of 10

millions of euros. Since a sanction is very serious, it should be twice as serious,

however, the very serious sanction is five times the serious one, reaching 100,000.00 euros

when double the grave would be 40,000.00 euros.

Taking into account that it is a non-profit administrative entity, it must be reduced to

at least a quarter, ranging between 25,000.00 euros for the very serious and

12,500.00 euros for the serious one, although this is said on a subsidiary basis, given that neither

there is an infraction, nor if there is, can it be sanctioned financially, being the right thing to do

with warning.

SEVENTH: On 03/21/2022, a test practice period begins, giving

reproduced for evidentiary purposes the filed claim and its documentation, the

documents obtained and generated during the claim admission phase, and

the report of previous investigative actions that are part of the procedure

E/08378/2020. Likewise, it is considered reproduced for evidentiary purposes, the allegations to the

agreement to initiate the aforementioned sanctioning procedure, presented by the claimed party and

the accompanying documentation.

In addition, the respondent is requested to provide and report:

a) System you are currently using to control working hours, and if you stopped

use the RF, date and accreditation of it.

On 04/04/2022, a response was received from the respondent indicating that "the system

current employee" is the cards, since he received the start agreement for "prudence" he

suspended the RF system on 09/08/2021, as soon as they acquired the cards. Provide invoice for

acquisition of 40 cards on 09/06/2021, type "RFID PAS radiofrequency proximity".

b) In the brief of the respondent dated 03/12/2020, it says that “Changing the

current timestamp system by one of face vectors, in which case it would store

a photograph as well as the system that was used with the cards”. Explain the meaning and

purpose of the underlined within the implanted RF system.

He states that what he means is that “there are no significant variations between the system

of cards and that of facial vectors, the purpose being to explain it to the delegates

XXXXXXXXXX. In any case, that letter only referred to a possibility

that was being shuffled. Therefore, when it is written, it is not yet known what it consists of.

really the system.

c) If the collection of facial images for registration was made with images (photographs)

of the employees previously used, or with the presence of the employees.

It states that with face-to-face action. “The same team that does the reconnaissance,

To do this, it previously captures the vectors that it is going to use on the employee himself. The

data or facial minutes, are captured, enter, are encrypted, are used by the device and do not leave

of it, without being able to be used for any other purpose, or extracted. The device only reports

externally to a single computer equipment of the entity: the date, time and name of the

verified person.

d) Identification of the technological support acquired for the technical operation of the system

And what does it consist of. Adding the elements that compose it, and if the services were contracted

system management with a provider. If the system has any type certification

ISO on biometric data. Copy of the data processing management contract by

charge.

It states that "a complete system was acquired, a compact unit, reading machine and

that processes the information and that carries its own program”. “The supplier does not have access or

was hired to manage anything in the system.”

In the invoice provided by document 2, it appears: 03/31/2020, equipment amounting to 375 euros

”SAFIER face control and facial access equipment, VSFTCT2MTFN3A “SOFTWARE

PRESENTIAL MANAGEMENT SAFIRE CONTROL CENTER” made in China, model SF-

AC3062KEMR-IP according to the brochure that is attached in document 4 in which the device is seen, and the

literal:

“Access and presence control- Facial recognition and EM card-1,600 faces, 2,500

cards and 50,000 registers, TCP/IP, USB and WIFI communication, integrated controller,

SAFIRE CONTROL CENTER AC software, Autonomous biometric reader for control of

Access."

It is also accompanied as part of the brochure the literal "specifications" that describes a

item description.

The image of the device “HIKVISION”, “DS-K1T9105 Series” is accompanied with the brochure

facial recognition terminal that informs that it works with a learning algorithm

can work as multiple authentication mode 1:N face pairing, IC

card authentication, etc. It also indicates the "characteristics"

On 04/26/2022, a GOOGLE search for “SAFIRE CONTROL CENTER AC SOFTWARE

existing among others the address:

“Safire Control Center AC Software

https://svtclti.com › manuals › SAFIRE-HIKVISION”, where by clicking the “manual

user SAFIRE CONTROL CENTER CONTROL access”. Title the manual version 2019 V1.0

build 07082019, of 114 pages in the pdf, which is incorporated into the procedure to complete

tests. On the same day, 04/26/2022, a copy of said access and the complete manual are sent to the

claimed. The manual contains the same aspects detailed in the brochures provided by the

claimed, detailing the system of operation and multiple and varied configurations

possible.

The manual, as well as the brochure that provides the claimed, informs that it has: sensor of activation auto activation by infrared, 2 MP camera with double sensor of facial recognition, TCP/IP communication, USB, RS485, Wi-Fi, Weight: 400 gr.-Modes of pin identification, card, facial recognition and combinations, integrated controller, bell push button door sensor and relay. It appears as an option to incorporate a photo as face, take a photo from the software, or capture faces from the camera control device. accesses, in order to verify if the facial recognition device administered in the software can recognize the face from the photo. The image of the compact device and a only piece of the user manual that provides the one claimed in document 4 “face recognition terminal” is a facial recognition terminal in which it is indicated that it “adopts algorithms deep learning, which help to recognize the face faster and with more certainty.

It also supports multiple authentication modes: 1:N face match, IC card authentication, etc. Note that the duration of facial recognition is no more than one second per person and the recognition accuracy rate is more than 99%.

e) Method of collection, registration and storage of the data of the employees used for the RF. Environment in which the system face comparison occurs and if there is a single point for it or several.

He states that "it is the equipment that takes the vectors", there is only one point and the environment is the equipment itself

f) Type of technology used for storage and operation of the RF, server, algorithm used and functions it performs.

"You buy the software that goes inside the equipment."

g) Regarding the reading of the data and positive identification, indicate the mode of operation and its synchronization, existing reading points of the data for the collation of the image and distribution in which these reading terminals are found. Specify, if when face is presented, where is the employee's stored template against which

the presented image is collated.? (if it is in the reader, in a database, features

of these.

He states that "there was only one reader at the entrance with the team that is also one." The team

It has the built-in program. The vectors are in the team, which is totally autonomous.

The entity only sees: day, time and identity of the verified person. Nobody can see anything else."

h) Indicate what happens if you do not recognize the face that is presented to you, and if you would store the template

of that person.

He states that nothing happens, because the device does not detect the vectors, he considers him not

logged and does not store anything.

Yo)

What connections does the computer database have with the data of the face that is

filed by employees, with employment data? Registry Association System

the face to the identity of the person. If the database is stored on servers, type of

server and location and ownership.

It states that it is not a computer as such, but "a fully integrated team, autonomous in its

functioning and independent. "To the assigned team of the ECE- the system only admits one-

the only information that arrives is the day, time and name or identity of the recognized employee

by the system."

j) Information system for each employee on the collection and processing of their data

provided, containing the purpose, legitimate basis and exercise of data rights

derivatives of the RF, and the way to prove its effective availability.

It states that it was reported at a staff meeting and they were ratified personally and

individualized when they went to take the photo, clarifying the questions, which in their case

could raise, which were few.

k) Accreditation that the time control system through the card was used

improperly.

States that the inappropriate use of time cards by some employees

it is not easy to prove this being the problem that allows fraud to be carried out in the registry

schedule without being detected. They provide document 5, a letter from an employee to the Governing Council,

and the agenda of the "personal assembly" of 02/18/2020 that contains at one point of the day

"information on the record of working hours" in which the matter that is

addressed this issue for allegedly passing another colleague's card on 01/30/2020 and

having received a reprimand, indicating "in relation to the assertions that some

companion has done", denies the facts, and states that when they were in line

several colleagues waiting in order in front of him, "he has given us his card and the

we have gone through the reader, but never without being present".

l) Copy of the time control record sheet generated by an employee in order to see the

data that is marked, and reported, if the system was also used for other people, or with

other purposes.

Indicates that the system was only used for the purpose of time recording. They accompany a

copy of a record of an anonymized employee as document number 6 appreciating

that for that person, the records can be grouped by days of the week, showing the

Hourly records noted with several entries and exits on some days.

m) Image sketch of spaces in which the devices for taking the video are located.

face for the registration of the day, explaining if there are interruptions of working time

effective and whether you have to re-register your face each time you enter or exit or

How would the pause system work?

It indicates that when the system was implemented, it did collect the stops or breaks because

contact with surfaces through the hands was not needed.

It states that there is only one device according to the accompanying sketch. “It is located in

a table, in a small room designed for this purpose, which is accessed from a patio by a

gate. It is appreciated that the system would be limited to presenting the face to the device and returning to

exit where you entered, as a presence record and that would capture date, time and data

of the employee.

n) Threshold value at which the software indicates that there has been a coincidence between the two

facial images that are compared, and what recommendation for this case does the manufacturer give.

Indicates that it is unknown, since “software was purchased from a third-party vendor.”

o) Copy of the record of treatment activities: "time control by acknowledgment

facial" in document 8, appearing as purpose: "time control of employees through

facial recognition”.

Legitimation: “existing employment contract with users. article 6. b) RGPD, obligation

legal requirement to register the working hours of employees, article 6.c), the need to

control of the workers: article 6. f), fulfillment through the personnel of the functions

of public interest entrusted: article 6.e)

“Categories of data minutiae of the face without output of the reading team day and time of reading

name and surname of the employee

Transfer of data: they are not foreseen except in the case of labor administration and labor courts.

Only data reported by the team

Storage period minimum four years, maximum 10 years, the data reported by the

reading team. Minutiae of the face, are eliminated at the end of the employment relationship.

Security measures: encryption of the minutiae of the face and watertight data retention

in the team.

p) From your point of view, what meaning do you give to the expression “biometric system

statistics" to which he alludes in some of his writings.

Indicates that this is information given by the manufacturer about how the treatment works.

Indicates that the system only collects specific minutiae or special characteristics, in

general position or dimensions of elements of the footprint or the face fundamentally

that do not allow to build the own imprint or the face of a person. It's about standing out

that the photograph of the person is not saved in the system but some special details and

with the statistical term that they are differentiating only within their own comparative group-

the entity's employees.

q) What interests and rights of employees, and security measures for their data are

taken into account in the establishment of the RF system.

It states that the interest for the establishment has been the health of the staff, taking the

measure in the context of a pandemic, confinement and fight against COVID, trying to avoid

infections derived from the use of palm cards.

As far as security measures are concerned, it is once again insisted that the device is watertight and

autonomous so there is no circulation of data or minutiae that the face takes.

In addition, it encrypts the data, so that it cannot be used by anyone, or for anything. The

apparatus takes the minutiae of the differentiating face, compared to the rest that has

of the group, encrypts them, and processes them, keeping them to make the identifications and only

reports the result, consisting of day, time and identity of the person, without these minutiae

circulate, nor are they used for anything, nor can they be used for other purposes.

r) Agreement approving the establishment of the RF system for time control.

Provides a copy of document 9, a certificate indicating that at the meeting of the Governing Council of

the Entity on 03/31/2020, the agreement of:

“The president informs that, given the expansion of the COVID-19 virus, and in order to avoid the

proliferation of contagions among the workers of this entity, who proceed daily to the

signing within their working day, another registration system would have to be determined.

After a long debate on the matter, it is unanimously agreed to proceed to the

acquisition of a facial biometric system for access control, thus eliminating the

possibility of any physical contact with said system.

s) Who is the owner of the facilities, urbanized public domain on which the

obligation to conserve of that entity, and if it took part in the decision to use the

RF.

Indicates that the owner of some of the facilities, such as the land and

buildings in which the offices of the entity itself are located is this same.

Other facilities such as roads, the sanitation network, green spaces, or

any facility or public domain space, are owned by the City Councils of

*** LOCATION.1 and from Nuevo Baztán.

“The City Councils did not participate in the decision-making, since they are part of the Council

but no vote.

t) What functions of the public ones that are attributed to it are exercised when deciding the use of

technical devices for the collection of data based on RF of the employees for their

time check.

It states that the conservation of public domain facilities of the

urbanization, which are put into practice and carried out through its employees of

in accordance with the bylaws of the entity.

They reiterate their consideration, already made in the allegations that it is the person, that is, the

entity as a public administrative entity and not the activity it carries out - which considers it

also public administrative - which determines the possibility of imposing a type of sanction

or another, without the possibility of making expansive interpretations on those established by law and

less to impose a sanction.

EIGHTH: On 05/03/2022, a resolution proposal is issued for the literal:

"That by the Director of the Spanish Agency for Data Protection is sanctioned with

warning to CONSERVATION COLLABORATING URBANISTIC ENTITY

EUROVILLAS, with NIF G79414033, for breaches of the RGPD:

-article 9.2.b) of the RGPD, typified in article 83.5 a) of the RGPD and in 72.1. e) of the

LOPDGDD.

-article 35 of the RGPD, typified in article 83.4 a) of the RGPD and in 73.t) of the

LOPDGDD."

Allegations are received on 05/17/2022, in which it indicates:

- The proposal does not explain what constitutes the unequivocal identification that makes the data

are considered special. To be before a special category of personal data,

we not only have to deal with biometric data, but with biometric data aimed at

unambiguously or uniquely identify a person. Not considered special data

means that no impact assessment is required.

unequivocal

- The statement that “they do not use images of faces, but

descriptions of these that are translated into certain patterns of the drawing of the face” and that the

system only takes “position or dimensions of the face that do not allow to reconstruct the face of

the person, which could coincide in many other people so they do not allow the

unequivocal identification of the subject, rather than within a small group of people such as

is the staff of the entity” “no unequivocal identifying data of any

employee". “In the procedure, an analysis or expert opinion has not been carried out on what captures

really the reader, being the burden of proof of that Agency, so it is not

accredited that what is stated in this part is not so”. “In this sense, rejecting the

inclusion in the file as evidence of the alleged User Manual located by the

instructor on the Internet through a generic Google search, having located the

same in a link in the main web address ***URL.1 (which does not return any results), for

not know if said Manual is correct, nor have they even complained to the manufacturer or

having confirmed its correctness with it. All facts and conclusions

carried out based on said Manual cannot be considered accredited or considered correct,

since it is not evidence obtained with due guarantees of veracity and certainty.”

-Reiterates that if there was a cause that lifted the prohibition of the treatment if the

same special data. “The letters g) and h) of article 9.2 of the RGPD by themselves, in a

individual and more put in relation between them with the own b) would justify the treatment”,

given the extraordinary pandemic situation experienced. “The letter h) fits better because it enables

treatment when it is necessary for purposes of preventive or occupational medicine”.

-Reiterates that it is not sufficient cause to state that before they controlled the working day with

cards, given the manipulation and fraud that have occurred "which have been explained and justified".

- “The alleged bases of legitimacy are rejected, considering that the claim is not justified.

use of a means that this Agency considers very intrusive, not keeping

proportionality, and because, in addition, previously, the control of the working day was done

by means of cards without justifying the problems that the same

presented”. “There is a legal basis for it, although that Agency ends up denying it in

based on an indeterminate legal principle: “that of proportionality”. “Proportionality”,

it is still something subjective and relative, not something clear and indubitable. You can discuss about

it. This party may accept that if the Agency considers it so, it is not justified

the treatment in attention to that judgment of proportionality between the interest of the Entity and the

employee rights, but it is quite another thing to impose a sanction.”

- It does not respond to the alleged situation, which was present at the time of the establishment of the

facial recognition, that of the extraordinary and serious health situation that endangered the

life and health of workers. Reiterates the importance of performing the functions of

employees when people spent more time than ever at home and that resulted

many affected employees, thereby wanting to prevent them from having to control the working day

with the fingerprint reader.

-Lack of guilt arising from the extraordinary and serious situation of the period in which

which the system was installed. They consider it to be non-existent. In addition, the resolution

indicates that it is the first resolution for the use of RF in the control of working hours.

PROVEN FACTS

1) On 03/12/2020, the respondent informs its 38 employees through their representatives

who, due to the coronavirus situation, is going to implement for the daily record of working hours

work day, the facial recognition (RF) system. On 04/30/2020, the respondent communicated her
establishment from 05/06/2020. Before the declaration of the pandemic, on 03/01/2020, the
The company had implemented the fingerprint system for the control of the lap time record.
labor, in the process of which he had informed the employees that the cards used previously
Previously, they were likely to be transferred to clock between employees on behalf of other
for the same function. The change to the RF, among other reasons, stated the respondent, was made
for avoiding contact with the fingerprint reader due to the spread of COVID.
2) The defendant is a collaborating conservation urban entity constituted with
obligatory character since 1988, grouping around four thousand owners, in some three thousand

single-family homes, forming a population of more than ten thousand inhabitants, according to the claim
madam).
3) The employees of the respondent provide in some cases a shift work regime, or
emergency services with attention 24 hours a day, and in addition, typical tasks related
with the purpose of the urban conservation entities: preserve the urbanization and the maintenance
maintenance of the endowments and installations of public services, by way of example:
zation of ordinary and extraordinary works and installations, tasks such as cleaning and wading
of streets, works to conserve and maintain, they can be roads (roads, sidewalks, parking)
and pedestrian network), sanitation network (collectors, sinks, treatment plants), sewage
rinsing, water supply (drinking, for irrigation, fire hydrants), supply
electricity (conduction, distribution and public lighting), and gardening and trees in
parks, gardens and public roads, furnishing and street furniture, for your use and enjoyment,

public ownership of the City Councils of ***LOCALIDAD.1 and ***LOCALIDAD.2 spaces

in which area the claimant is located.

The respondent adopted on 03/31/2020, the agreement to record the daily working day for

employees of your entity, through the use of an RF biometric system, taking into account

account the expansion of COVID-19, and in avoiding the proliferation of infections among

workers. The claimant states in the transfer that the RF is “the most suitable for

guarantee the health of workers”, “effective and proportional” without documentation that

support these claims.

4) In the register of activities of the treatment of the claimed, it appears: "time control by re-

facial knowledge” purpose: “time control of employees through fa-

cial”.

Legitimation: "existing employment contract with users article 6. b) RGPD, legal obligation

of registering the working hours of employees (article 6.c), the need to

control of the workers (article 6. f), fulfillment through the personnel of the functions

of public interest entrusted: article 6.e)”

“Data categories: minutiae of the face -without exit from the reading equipment-. day and time of

reading name and surname of the employee”.

Transfer of data: they are not foreseen except in the case of labor administration and labor courts-

only data reported by the team.

Storage period; minimum four years, maximum 10 years, the data reported by the

reading team. Minutiae of the face, are eliminated at the end of the employment relationship.

Security measures: encryption of the minutiae of the face and watertight data retention

in the team."

5) The device used by the claimed person was acquired on 03/30/2020, according to its manual, designed

do for face-to-face control and facial access, SAFIER, model SF-AC3062KEMR-IP, manufactured

in China “ 1,600 faces, 2,500 cards and 50,000 registers, TCP/IP, USB and WIFI, controller

integrated, Safire Control Center AC Software, recognition time, <0.5 sec., weight 400 gr,

2 MP camera with dual facial recognition sensor, 5 LCD touch screen, a cost of

375 euros. It appears as options, those of incorporating a photo as a face, taking a photo

of the software or capture faces from the access control device, in order to ve-

verify whether the facial recognition device managed in the software can recognize the

face from photo The image of the device provided by the claimed one is a recovery terminal

facial recognition stating that it “adopts deep learning algorithms, which

they help to recognize the face faster and with more certainty”. It also supports modes of

multiple authentication: 1:N face match, IC card authentication, etc.

The facial recognition device is installed on a computer protected with

password, to which only one person has access, the biometric data being encrypted,

not being removable. The device that carries its own software inside does its own

extract landmarks from the face after taking the picture and create a pattern. The

device has only one reader. Provides the computer of the claimed reports

on time, date and employee on each occasion that enters and leaves, for which you have to

go through the room in which the image capture occurs.

6) Technically, from the information extracted from the file, by communication of the claimed

to claimant, statements of the claimed, and documents provided, the RF system

for purposes of daily registration of working hours consists of a device placed in a

room in front of which the employees present the face and through the RF, records the time,

date and name and surname of the employee.

The software system works by extracting two-dimensional images of the face, not
preserves images or photographs of the face, but translates the taking of the photograph that
company made the employees in person to a template, with the characteristics of
the captured parameters, template that is saved in the equipment or system linked to the
name and surname of the employee. When a biometric sample of the person is captured,
when entering or exiting work, compares it with the registered templates and outputs the
time, date and the name and employee of the person who enters or leaves the day shift. In
Every time the employee has to make a break in the day, he must return to
enter the room and present the face for registration. The processed data is
on the entity's servers. According to the claim, the registered data is
stored on the same device where the registration takes place.

7) The respondent has not provided the AEPD with an assessment of the impact of data processing
RF biometrics for the registration of the daily working day of its employees, alleging
that does not process biometric data of a special nature because they do not uniquely identify
a person.

8) On information to those affected by the collection and processing of their data, containing
the purpose, legitimizing basis and exercise of rights derived from the treatment of recognition
facial treatment for the daily record of the working day, said the respondent who was informed
at a staff meeting and when they stopped by to take their picture. Figure that the claimed, in
document 6 provided by the claimant, on 04/30/2020, informs her of the implementation of the RF:
”This system works from the identification of a percentage of characteristics extracted
das of the face, without taking a three-dimensional image of the faces, we understand that this
This measure is less invasive than the recording of the moment of signing by camera, which also
more involved physical contact with a shared card reader. The sole purpose of these data
is the signing of personnel and analysis of work times for compliance with the decree

Law 8/2019, in order to analyze the data in decision-making and the defense of their interests.

be legitimate.” “These data will be found on the servers of this entity, in no case

on the cloud". On the occasion of the implantation of the previous fingerprint system for the same

purposes, the parties had exchanged writings on the use, purposes and information and con-

The claimant's disagreement with the system was evident.

9) On 09/17/2021, in pleadings to the agreement, the respondent indicated that “it has become

to the card transfer system” since receiving the initial agreement, providing an invoice

purchase of these items.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of

control, and according to the provisions of articles 47 and 48 of the LOPDGDD, the Director of the

Spanish Agency for Data Protection is competent to initiate and resolve this

process.

II

The regulatory adjustment that is analyzed in terms of

to the RF system for the daily record of working hours that the respondent acknowledges has

implemented and used from 05/06/2020, until receiving the start-up agreement, with the purpose of

process the data of the 38 employees of your entity for the daily record of the working day,

obligation imposed in article 34.9 of the Consolidated Text of the Law of the Statute of

Workers, approved by Royal Legislative Decree 2/2015, of 10/23 (ET).

Strictly speaking, this is not the first type of claim that has been

had input in this AEPD, some having already been resolved. However, if it is

of the first related to data processing as an employing entity that decides

use the registration and storage of data originated by the RF for the purpose of registration

working day diary.

The scope of application of the RGPD extends its protection, as established in its article 1.2,

to the fundamental rights and freedoms of natural persons and, in particular, their 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 party"); person will be considered

identifiable physical person any person whose identity can be determined, directly or indirectly,

in particular by means of an identifier, such as a name, a number of

identification, location data, an online identifier, or one or more elements

inherent to the physical, physiological, genetic, mental, economic, cultural or social identity of

said person."

The right and ownership of the personal data that each person recognized in the article

18.4 of the Spanish Constitution, was interpreted in the ruling of the Constitutional Court

292/2000 specifying that:

"This fundamental right to data protection…attributes to its holder a bundle of

powers consisting for the most part in the legal power to impose on third parties the

performance or omission of certain behaviors whose specific regulation must

establish the Law, the one that according to art. 18.4 CE must limit the use of information technology,

either developing the fundamental right to data protection (art. 81.1 CE), or

regulating its exercise (art. 53.1 CE). “

“The fundamental right to data protection seeks to guarantee that person a

power of control over your personal data, over its use and destination, for the purpose of

prevent their illicit and harmful traffic to the dignity and rights of the affected party. … The right to

data protection guarantees individuals a power of disposition over these data. Is

guarantee imposes on the public authorities the prohibition that they become sources of that

information without due guarantees; and also the duty to prevent risks that may

arising from improper access or disclosure of such information. But that power

provision on the personal data itself nothing is worth if the affected party does not know what data

are those owned by third parties, who owns them, and for what purpose. “

As specific types, biometric data is defined in article 4.14 of the RGPD:

"biometric data": personal data obtained from a specific technical treatment,

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

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

fingerprint data;

To be considered biometric data in the sense of the RGPD, the processing of data without pro-

cease, such as the physical, physiological or behavioral characteristics of a natural person de-

may involve a measurement of those characteristics. Since biometric data is the

result of such measurements, the RGPD indicates in its article 4, section 14, that they are data

personal “[…] obtained from a specific technical treatment, related to the characteristics

physical, physiological or behavioral characteristics of a natural person that allow or confirm

the unique identification of said person [...] »Thus, from the concept, we must not lose sight of the

ta:

-The nature of the data: data relating to the physical, physiological or

conduct of a natural person;

- The means and forms of treatment: data "obtained from a treatment

specific technician'; what differentiates, for example, from the images of a person who figures ran in a video surveillance system, which cannot be considered biometric data if it is not have been technically treated in a specific way in order to contribute to the identification unique to that person. Recital 51 of the RGPD also refers to the non-consideration systematically as a special category treatment of data, to photographs, to me- us that a specific technical treatment means be applied to them that “allows the identification unequivocal authorization or authentication of a natural person”.

- The purpose of the treatment: the data must be used for the purpose of identifying uniquely to a natural person.

Biometric data have the peculiarity of being produced by the body itself and definitively characterize, they are data not about that person, but the data refers to the same person, in principle not modifiable by the will of the individual, nor can the person be released from them, they cannot be changed in case of compromise-loss or intrusion into the system. In addition, because biometric data is unique to a person and

perpetual, the user uses the same data in different systems. Therefore, a robbery identity is not only perpetual in time, but also affects all systems in which a user has their biometric data stored. The holder therefore does not have the possibility to use a biometric data for the bank, and a different one for your health system, but that uses the same information to verify your identity in both, and against a vulnerability are affected all of them at the same time. Finally, the interested party does not know finds out that your information is being used, being able to obtain it through objects,

traces or surveillance cameras.

Also from the start, it is necessary to highlight the note of the restrictive nature, since in principle, its treatment is prohibited and can only be treated exceptionally, in certain assumptions that are contemplated in the RGPD, which provides strict requirements for finally enable the commissioning of such systems, due to the affectation to fundamental rights and freedoms, due to the risks that may entail the context of their treatment, and that as stated in Recital 51 of the RGPD: "Such personal data does not must be treated, unless treatment is permitted in specific situations referred to in this Regulation, taking into account that the Member States may establish 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 to the fulfillment of a mission carried out in the public interest or in the exercise of powers data conferred on the data controller. In addition to the specific requirements of such treatment, the general principles and other rules of this Regulation, especially in what refers to the conditions of legality of the treatment. I know should explicitly establish exceptions to the general prohibition of data processing. those special categories of personal data, among other things when the interested party gives your 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 freedoms fundamental."

Considering (52) "Also, exceptions must be authorized to the prohibition of treating special categories of personal data when established by the Law of the Union or of Member States and provided that the appropriate guarantees are given, in order to protect data personal and other fundamental rights, when it is in the public interest, in particular:

- the processing of personal data in the field of labor law,

- legislation on social protection, including pensions and

-for security, supervision and health alert purposes, the prevention or control of

communicable diseases and other serious threats to health. (...)”

III

The defendant has processed personal data, and specifically biometric data. The

concept of treatment The RGPD defines in its article 4:

“2) «processing»: any operation or set of operations performed on data

personal data or sets of personal data, whether by automated procedures or not,

such as the collection, registration, organization, structuring, conservation, adaptation or

modification, extraction, consultation, use, communication by transmission, diffusion or

any other form of authorization of access, collation or interconnection, limitation, suppression or

destruction;

7) “controller” or “controller”: the natural or legal person, authority

public, service or other body that, alone or jointly with others, determines the ends and means of the

treatment; if the law of the Union or of the Member States determines the purposes and

means of treatment, the person responsible for treatment or the specific criteria for its

appointment may be established by the Law of the Union or of the Member States;

The definition of biometric data refers to "technical treatment", without specifying, except for

Note that the purpose of such processing must be to identify a person. The

biometric characteristics are subjected to a technical treatment through a process that is

contains in all biometric data processing: data capture or registration,

storage or processing and last phase of comparison.

The photographs of the employees are captured obtaining an image, from which they are extracted the characteristics through the algorithm, which is part of the software of the device of the claimed. These characteristics-facial vectors, the claimed one calls them- are the measurements positioning and relative reference measurements (nodal points distance: between the eyes, shape of cheekbones...) that collects from each image in each individual and the point of natural starting point for the treatment and automatic recognition of individuals. The Feature extraction provides information to distinguish between faces.

of different people according to their geometric or photometric variations.

The raw image of the biometric characteristics is reduced,

transforming,

conserving outstanding discriminated information that is essential for the recognition of the person. These extracted characteristics are kept in a biometric template, which it is a form of reduced mathematical representation of the original characteristic. Template reference is stored for comparison. In the last phase, a sample will be compared biometric -such as the face- presented to the sensor with a previously recorded template. The phases agree with the enumeration of what could be a treatment operation of data (collection, storage, use). The operation of the fingerprint is similar, with unremarkable nuances because they do not fundamentally vary the mode of operation.

The non-reference to its assessment in this procedure cannot be assessed as intended. the one claimed in his allegations.

As for the fact that it only identifies those belonging to the group of employees, that is no reason to not be considered biometric data, which are aimed at natural persons being identify with the data generated from the extraction of its characteristics biometrics

Regarding the consideration of biometric data as special data, it is necessary to take into account

Note that in the proposals on the Data Protection reform package, which

led to the approval of the RGPD, the European Commission, only added to the list of data

sensitive, genetic data. It was the European Parliament that added to the list of data

sensitive, biometrics, when he voted for the GDPR proposal on 03/14/2014, despite the fact that

some national authorities suggested, due to their specific nature, to add them to the list of

sensitive data.

On the one hand, the definition of biometric data includes that through the technical treatment

specifically, “enable or confirm” the “unique identification” of said person. mentions to

“allow” can be understood as identification, “confirm” as verification. So,

both, identification or authentication must be unique, referring to the identification that is

produce of the person. Unique identification, on the other hand, goes beyond the fact that the data is

of an identified or identifiable natural person. Data of the identified natural person is that

that person is distinguished or isolated from a group of people. Unique, may refer to the

biometric data have such particularities that they can unambiguously identify a

individual

The differences between the terms identification-authentication refer to the way of

search in the stored records and to the previous entry of the record, as can be deduced

of Opinion 3/2012, of WG 29, of 04/27/2012, on the evolution of technologies

biometric data, at a time when biometric data did not enjoy the category of

“special” that the RGPD introduces and therefore the term “aimed at the

unique identification. The opinion differentiated between:

“Biometric identification: the identification of an individual by a biometric system is

typically the process of matching your biometric data (acquired at the time of

identification) with a series of biometric templates stored in a database (it is

i.e. a one-to-many mapping process).

Biometric verification/authentication: the verification of an individual by a biometric system

is normally the process of comparing your biometric data (acquired in the

time of verification) with a single biometric template stored on a device

(i.e., a one-to-one mapping process).”

Recital 51 states that “The treatment of photographs should not be considered

systematic processing of special categories of personal data, since

are only included in the definition of biometric data when the

The fact of being treated with specific technical means allows the identification or

unequivocal authentication of a natural person. Such personal data must not be processed,

unless their treatment is allowed in specific situations contemplated in the

this Regulation”.

Article 9.1 together with the prohibition of treatment indicates that they are, those "aimed at identifying

uniquely to a natural person”, which indicates that the biometric data, for

nature, they are not sensitive, but will depend on the use or context in which they are used, the

techniques used for their treatment, and the consequent interference in the right to

Data Protection.

Technically, the biometric template against which the sample is checked is the product of

a measurement that uniquely and uniquely identifies the individual. This is what for example

differentiates the images viewed from a camcorder that cannot be considered

biometric data under the definition of article 9 if they are not specifically treated with a

technical means to contribute to the identification of a person.

The biometric data of each employee, acquired at the time of capture, is

relate to the name and surname of the employee who registers them, to submit them to the technical procedure that converts the image, the format, into a biometric sample and the algorithm in biometric template, being stored, so that with the samples introduced to the sign in, they are compared with the series of biometric templates stored in the database, that is, the comparison does not occur with a single biometric template stored in the

device. Facial recognition is not only capable of accurately validating identity, instead, it has unique information about natural persons. The algorithm of the software, on the biometric sample, extract biometric characteristics, reduce and transform into label or numbers that sample, constituting a mathematical representation of the characteristic original biometric, which is the biometric template. The template is stored for your comparison in the last phase in which with the biometric sample-face-and with the template previously recorded, is uniquely identifying the employee, each time he enters or leaves by lending your face to the device, so the data is considered to enter within the scope of special data.

In the present case, of course, it cannot be said that information linked to personal data of a person identified in each time record, although the data is stored on the device encrypted/encrypted. Every time an employee stands in front of the camera, allows or confirms its unique identification through the treatment carried out by the claimant with the purchased device. The presented sample is compared and the system has the identification function with a biometric function, uniquely identifying the employee who claims to be and registering their data. On the allegation that the system only takes

“position or dimensions of the face that do not allow to reconstruct the face of the person, the
which could coincide in many other people so they do not allow the identification
unequivocal of the subject, rather than within a small group of people such as the staff
of the entity” “no unequivocal identification data of any worker is kept”, it must be
point out that if they did not allow the unequivocal identification of the employee, the
registration that has been carried out, of which the respondent has not accounted for any
irregularity in the records carried out with your system, or you would not have passed the
acceptance threshold of the device and would not access with the consequent lack of annotation,
as happens if the registered pattern does not match. Otherwise, it has been detailed
consistent operation in the technical transformation of the biometric trait that allows the
unique identification even within the small group of employees.

Regarding the incorporation of the user manual, of which a complete copy was sent, no
can accept the allegation of lack of certainty, since it is a reflection of the specifications
that are detailed in the brochures that the claimant sends, without the claimed having provided the
that if it considers true or truthful. The specificities indicated in the manual coincide with the
details that it gives of the autonomous system that it uses as software and that appear in the brochures
sent in evidence by the claimed. Available technology plays a determining role
in the identification of the person (recital 26 of the RGPD) and therefore it must be mentioned
and bring this manual to the case, even if it is to appreciate its general characteristics. On
the lack of expertise that verifies that the system works as claimed, it is not
You can argue that initially a photograph of the employee is taken, identifying with their
employee data correlating your template, being true that it is about the image
processed on which is produced through its capture a biometric sample and a
staff, there being no differences in terms of its consideration, which is per se a
data treatment.

IV

Article 7 of the Charter of Fundamental Rights prescribes that everyone has
right to respect for their private life, and article 8.1 that every person has the right to
protection of personal data that concerns you. Performed together,
infers that any data processing may constitute a violation of such rights.
by a third party, in this case the claimed party. This use of the data of your
employees, whose ownership corresponds to them, could suppose a violation of their right to
privacy and data protection if it is not justified. Article 8.2 of the Charter
of Fundamental Rights specifies that personal data can only be
processed with the consent of the interested party or by virtue of another legitimate basis provided
by Law. In addition, articles 7 and 8 of the charter are not absolute, admitting limitations,
provided that they are provided for by law, respect the essential content of those rights and
with observance of the principle of proportionality, are necessary and respond
effectively to objectives of general interest recognized by the Union or to the need to
protection of the rights and freedoms of others (Decision of the Court of Justice of the
European Union, fourth room, judgment of October 15, 2013, C/291/2012.). These
other aspects, are reiterated in relation to fundamental rights, in art.
52.1 in fine of the Charter of Fundamental Rights of the EU.

The defendant is charged with the infringement of article 9.2.b) of the RGPD.

Article 9.1 of the RGPD indicates:

“Treatment of special categories of personal data”

1. The processing of personal data that reveals ethnic origin or

racial, political, religious or philosophical convictions, or trade union membership, and

the processing of genetic data, biometric data aimed at uniquely identifying

to a natural person, data relating to health or data relating to sexual life or

sexual orientation of a natural person.

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

following:

[…]"

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

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

Labor law and security and social protection, to the extent authorized by the

Law of the Union or of the Member States or a collective agreement pursuant to

Law of the Member States that establishes adequate guarantees of respect for the

fundamental rights and the interests of the interested party;

c) the treatment is necessary to protect the vital interests of the interested party or another

natural person, in the event that the interested party is not capable, physically or legally,

to give your consent;

[…]"

g) the processing is necessary for reasons of essential public interest, based on the

Law of the Union or of the Member States, which must be proportional to the objective

pursued, essentially respect the right to data protection and establish measures

adequate and specific to protect the interests and fundamental rights of the

interested;

But when it comes to biometric data, in addition to lifting the ban on their processing,

must contain one of the legal bases legitimizing the treatment contained in the

article 6.1 of the RGPD. The fundamental right to data protection, provided for in the

Article 18.4 of the EC, is based, as regards the case, on the essential principle that the

data processing of its owner, "it will only be lawful if at least one" of the

conditions provided for in article 6.1.a) to f) of the RGPD, on the basis that any

treatment of these data restricts the rights of its owner by the mere fact of suffering such

treatment, moment from which each time it will be identified with this mechanism.

The respondent alludes in her treatment record to three bases of legitimation, which proceeds

examine separately:

- “the treatment is necessary for the execution of a contract in which the interested party is

part or for the application at the request of the latter of pre-contractual measures;” article 6.1. b) GDPR,

adding that it also concurs that of article 6.1.c) of the RGPD "The treatment is necessary

for the fulfillment of a legal obligation applicable to the data controller”.

The legal obligation to record working hours does not derive from obligations assumed between

the parties but of legal regulations contained in article 34.9 of the ET, which provides:

“The company will guarantee the daily record of the working day, which must include the specific hours of

start and end of the working day of each worker, without prejudice to the

time flexibility established in this article.

By collective bargaining or company agreement or, failing that, by decision of the

employer after consultation with the legal representatives of the workers in the company,

this day record will be organized and documented.

The company will keep the records referred to in this provision for four years and

will remain at the disposal of the workers, their legal representatives and

the Labor and Social Security Inspection.”

For control through the daily record of the working day of each employee, it is necessary treat your data. Different is the analysis of necessity and proportionality in the middle chosen, for which it could be considered that there are alternative systems.

The Article 29 Working Group, GT29 (adopted on 06/08/2017) (created by virtue of the Article 29 of Directive 95/46/EC, European independent advisory body on the subject of data protection and right to privacy, whose tasks are described in article 30 of Directive 95/46/CE and in article 15 of Directive 2002/58/CE, assumed today by the European Committee for Data Protection, CEPD), in its Opinion 3/2012 on the evolution of biometric technologies, indicates that "When analyzing the proportionality of a system proposed biometric, it is necessary to consider beforehand if the system is necessary to respond to the identified need, 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 will be effective in responding to the need in question in the light of 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 benefits

expected. If the benefit is relatively minor, such as increased comfort or a slight savings, then the loss of privacy is not appropriate. The fourth aspect to evaluate the suitability of a biometric system is to consider whether a less invasive means of intimacy would achieve the desired end.

It must be considered that in this case, prior to the establishment of the RF, the entity had with cards to control working hours, although it does not seem to have analyzed other alternatives of

use for that purpose.

- Another basis of legitimacy provided by the claimant is the "need to control the

workers", 6.1 f) of the RGPD, when the RGPD defines that article, as: "the treatment is

necessary for the satisfaction of legitimate interests pursued by the person responsible for the

treatment or by a third party, provided that the interests do not prevail over said interests.

or the fundamental rights and freedoms of the interested party that require the protection of

personal data, in particular when the interested party is a child.", extreme that of all

modes does not develop or develop the balance of the prevalence of rights and interests,

It should be added that this legal basis does not apply as the drafting of the aforementioned continues.

precept "… to the treatment carried out by public authorities in the exercise of their

functions.", considering that as a public entity it performs said functions by delegation.

- Finally, the "compliance through the personnel of the functions of public interest

entrusted", article 6.1.e) of the RGPD, which actually indicates: "e) the treatment is

necessary for the fulfillment of a mission carried out in the public interest or in the exercise of

public powers conferred on the data controller", would not be applicable either,

since article 8.2 of the LOPDGDD establishes that the processing of personal data only

may be considered based on the fulfillment of a mission carried out in the public interest or

in the exercise of public powers conferred on the controller, when derived from a

competence attributed by a regulation with the force of law.

Thus, the only base that could be applicable would be 6.1.c).

However, resorting to the lifting of the ban that provides for the treatment of

biometric data, article 9.2.b) of the RGPD, which is the one related to the scope

employment, determines that:

- the treatment must be necessary for such compliance,

-to the extent authorized by the Member States,

- or a Collective Agreement also in accordance with the law of the Member States, which

establish adequate guarantees of respect for fundamental rights and interests

Of the interested.

These are cumulative requirements that represent an additional guarantee in the treatment of damages.

rights of its owner, which takes into account that if the achievement of the intended purposes can be

be processed without the processing of personal data, this route will be preferable and will mean that it is not necessary

necessary to carry out any treatment of data, and subsidiarily, that the collection of data

is necessary for the stated or intended purpose and, if so, that it is proportionate.

nal.

In any case, in these treatments, one must be very cautious in the assessment that is made.

made as to whether these requirements are met, since special data is being processed.

Subsidiarily, the defendant points out, other literals of article 9.2 of the RGPD, none of

they reach to lift the presumption of the prohibition of the processing of biometric data,

by:

- Article 9.2.g): “processing is necessary for reasons of public interest

essential”, since a public interest does not legitimize any type of data processing

personal, but must be, in the first place, to the conditions that have been able

establish the legislator, as provided for in article 6 of the RGPD, in its sections 2 and 3,

as well as the aforementioned principles of article 5 of the RGPD, especially those of limitation

of the purpose and minimization of data. In this case, there is no rule that provides for the

statement of essential public interest in the processing of facial image data

for the labor registry, nor the guarantees that should be carried with that declaration.

-that the "treatment is necessary for purposes of preventive or occupational medicine", that it does not bears no relation to the installation of the device for records, within a context of a pandemic in which the right to data protection is not suspended, providing the personal data protection regulations and the applicable sector of a regulation for such cases that reconciles and weighs the interests and rights at stake for the common good.

Thus, it is concluded that the cause of legitimacy to carry out the time control of the day daily work, only reaches the obligation to carry it out, but not to carry it out using data biometrics, and their use, without cause of exception for the treatment, as has been accredited, It supposes the infringement of article 9.2.b) of the RGPD.

v

The breach of article 9.2.b) of the RGPD of the claimed party, is described in the ar-Article 83.5.a) of the RGPD, with the reference:

“The infractions of the following dispositions will be sanctioned, in accordance with the section 2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of a company, of an amount equivalent to a maximum of 4% of the total turnover annual global of the previous financial year, opting for the highest amount:

a) the basic principles for treatment, including the conditions for consent pursuant to articles 5, 6, 7 and 9;”

The LOPDGDD establishes in its article 72.1.e) of the LOPDGDD:

"1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679, it is considered They will be very serious and will prescribe after three years the infractions that suppose a violation substantial modification of the articles mentioned therein and, in particular, the following:

“e) The processing of personal data of the categories referred to in article 9 of Regulation (EU) 2016/679, without any of the circumstances provided for in said precept and in article 9 of this organic law.”

Opinion 2/2017 on data processing at work, of WG 29, establishes that

“Regardless of the legal basis for such processing, prior to its commencement,

perform a proportionality test in order to determine whether the treatment is

necessary to achieve a legitimate purpose, as well as the measures to be taken to

guarantee that violations of the rights to privacy and secrecy of

communications are kept to a minimum

Since in the 90s of the last century our Constitutional Court adopted the

called the "German test" in the examination of the principle of proportionality, is a constant

in its jurisprudence, that the measures that affect fundamental rights must be

suitable or adequate, necessary and proportionate in the strict sense.

Section 72 of Guidelines 3/2019 on the processing of personal data through

video devices, of January 29, 2020, of the CEPD, indicates: "The use of data

biometrics and, in particular, facial recognition entail high risks for

rights of the interested parties. It is essential that the use of such technologies have

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, data controllers

must first assess the impact on fundamental rights and freedoms and

consider less intrusive means of achieving your legitimate purpose of processing. " Namely,

the question of whether this biometric application is something that really is

essential and necessary, or is it just “convenient”.

Opinion 3/2012, on the evolution of biometric technologies of 04/27/2012, of the WG 29, indicates that: “When analyzing the proportionality of a proposed biometric system, it is It is necessary to consider beforehand if the system is necessary to respond to the need identified, that is, if it is essential to satisfy that need, and not just the most adequate or profitable. A second factor that must be taken into account is the probability of 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 benefits expected. If the benefit is relatively minor, such as increased comfort or a slight savings, then the loss of privacy is not appropriate. The fourth aspect to evaluate the suitability 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, but considering the risks of using a intrusive technology, bias, or the likelihood of misidentification, your interoperability, identity theft and the type of identity unique, permanent and invariably dealt with, its impact on the privacy of individuals, the implications on fundamental rights issue of such systems and security measures, Their use increasingly widespread, and technological interconnection is more likely to interfere with these fundamental rights and can lead to a serious violation of rights.

can lead to serious violation of rights.

Data controllers must ensure that the assessment of the need and the proportionality consider a thorough assessment of alternative options less intrusive available. Therefore, the feasibility of other options needs to be documented available alternatives that do not require the use of special data, compare all the

options and document the conclusions. All this, considering the context of the framework in

which the treatment is traced, the fulfillment of the obligations through the registration of

working day.

Necessity implies that a combined, fact-based assessment of

the effectiveness of the measure for the objective pursued and whether it is less intrusive in

comparison with other options to achieve the same goal

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

than carrying a card, it is automatic and instantaneous and not excessively expensive.

Obviously, an RF system can be useful, but it doesn't have to be objectively

necessary (the latter being what really must be present). As it establishes

opinion 3/2012 on the evolution of biometric technologies - of WG 29 -, must

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

profitable". Regarding the reliability of the system, it must be said that the greater the

number of identification systems that are based on biometric data or a template

obtained from biometric data, the greater the risk that this data may end up

being used improperly and giving rise to a risk of usurpation or

identity fraud.

Regarding the production of these impersonation events, the respondent contributed a

example of a single case that occurred two months before implanting the first means of

Fingerprint time control. It is a letter from an employee who does not prove

reliably that the aforementioned impersonation had occurred in the use of credit cards

according to their statements and the lack of a procedure based on accrediting the facts, which is not provided. The allegation that the use of the facial recognition because it previously used the card system, it is not mentioned in the proposal. In any case, it can be concluded that such fraudulent uses are not accredited. by the mention of a case, which, as is proven, are statements by the employee. In addition, an internal sanctioning system could be established that discourages and is cash for the fraudulent use if it were the case of the cards, it is not justified that the treatment through the RF is necessary for the fulfillment of the obligations in labor matters such as the record of daily working hours established by law.

Mention anyway that you have returned after the start agreement to that system and have to analyze the options and alternatives before establishing a new system that supposes a exaggerated limitation of the right of each employee, when there may be less invasive of intimacy, and not opting for what is practical and comfortable when they are at stake rights of their owners. The risks of treatment must also be considered, which denote a lack of full consolidation of confidence in the system, given the pros and cons cons, being aware that biometric systems can be circumvented and be compromised your data and information, in relatively easy ways. In this case, the type of activity, common to many companies, such as the registration of working hours, cannot give foot to the treatment of special data in group blocks, which do not generate more advantages or benefits for the general interest than damages on the goods or values in conflict. It is reiterated that given the purpose to be achieved and the legal assets in takes place, the context in which it occurs, the type of activity carried out by the claimant, which does not entail a significant risk to protect or a supreme or prevalent legal right, it supposes that the specialized treatment that it proposes cannot give way for the registration of working hours, influencing the judgment of proportionality, as outlined in Opinion 3/12 on the evolution of biometric technologies.

7th

In addition, the proactive responsibility system implemented by the RGPD, focused on the continuous management of the potential risks associated with the treatment, imposes on the responsible for the treatment that analyze what data they process, for what purposes and what type of treatments carried out, relating the potential risks to which they are exposed and from there, decide what measures to take and apply to ensure compliance based on tion of the risks detected and assumed.

RF processing poses high risks to fundamental rights and freedoms and before implementing a data processing project, as long as it is likely that it poses a significant risk to the rights and freedoms of individuals, as in this case, it is necessary to audit its operation, not in an isolated way but in the context of the specific treatment in which it will be used. The impact evaluation in the protection of personal data, EIPD, is the tool that in the RGPD deals with the guarantee of compliance with this aspect of the treatment.

In this case, the various risks that may occur must be analyzed, including their technology, within the framework of an increasingly intensive use of this type of data. Its use, interoperability and technological interconnection, is more than likely to interfere with these fundamental rights and may give rise to questions about its implementation.

The RGPD establishes the obligation to manage the risk that for the rights and freedoms of people involves treatment. This risk arises both from the very existence of the treatment, as well as its technical and organizational dimensions. The risk arises

for the purposes of the treatment and its nature, and also for its scope and the context in which that unfolds

The use of biometric data and, in particular, the RF entails greater risks for the rights of the interested parties. It is essential that the use of these technologies be made duly respecting the principles of legality, necessity, proportionality and minimization of the data established in the RGPD. Although the use of these technologies may be perceived as particularly effective, those responsible must, first of all, assess the impact on fundamental rights and freedoms and consider less intrusive to achieve its legitimate purpose of processing.

The “risk-based approach” is developed in the “Statement on the role of a risk-based approach in data protection legal frameworks WP218” of WG 29, WP218, and is not a novel concept in the framework of data protection.

Risk management for rights and freedoms, aims to study the impact and the probability of causing harm to people, individually or socially, as consequence of personal data processing. In contrast, risk management of regulatory compliance aims to provide the person in charge with a tool to verify the degree of compliance with the obligations and precepts legally required with in relation to a treatment activity. Therefore, prior to the management process of risks and as a sine qua non condition to undertake a treatment activity, it is

It is necessary to systematize the verification of regulatory compliance throughout the entire cycle of treatment life. The complexity of the risk management process has to be adjusted, not to the size of the entity, the availability of resources, its specialty or sector,

but to the possible impact of the treatment activity on the interested parties and to the own

treatment difficulty.

Article 35 of the RGPD whose infringement is attributed to the claimed one, establishes the obligation to

have an Impact Assessment on the Protection of Personal Data (EIPD),

pointing out:

"1. When a type of treatment, particularly if it uses new technologies, is likely to

gies, 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 will carry out, before the treatment

treatment, an assessment of the impact of processing operations on the protection of

personal information. A single assessment may address a number of treatment operations.

similar transactions involving similar high risks.

2. The person in charge of the treatment will obtain the advice of the delegate of protection of

data, if appointed, when conducting the data protection impact assessment.

data.

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

1 will be required in particular in case of:

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

based on automated processing, such as profiling, and on the basis of which

take decisions that produce legal effects for natural persons or that affect them

have significantly similarly;

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

9, paragraph 1, or personal data related to criminal convictions and offenses to

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 of

treatment that require an impact assessment related to data protection of

in accordance with paragraph 1. The supervisory authority shall communicate these lists to the Committee at

referred to in article 68.

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

that do not require data protection impact assessments. the au-

The Control Authority shall communicate these lists to the Committee.

6. Before adopting the lists referred to in sections 4 and 5, the supervisory authority

authority shall apply the consistency mechanism provided for in Article 63 if those lists

These include treatment activities that are related to the offer of goods or services.

services to interested parties or with the observation of their behavior in several States

limbs, or treatment activities that may substantially affect the free movement of

transfer of personal data in the Union.

7. The evaluation must include at least:

a) a systematic description of the processing operations envisaged and of the purposes of the processing.

treatment, including, where appropriate, the legitimate interest pursued by the person responsible for the

treatment;

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

with respect to its purpose;

c) an assessment of the risks to the rights and freedoms of the interested parties to which

refers to section 1, and

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

and mechanisms that guarantee the protection of personal data, and to demonstrate conformity
with this Regulation, taking into account the rights and legitimate interests of
stakeholders and other affected persons.
8. Compliance with the approved codes of conduct referred to in article 40 by
those responsible or in charge will be duly taken into account when assessing
Evaluate the repercussions of the treatment operations carried out by said controllers
or entrusted, in particular for the purposes of the impact assessment relating to the protection of
data.
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 interests
public or commercial 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 that applies
that the person responsible for the treatment, such Law regulates the specific treatment operation.
or set of operations in question, and an impact assessment has already been carried out
on data protection as part of an overall impact assessment on the
context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply
except if the Member States consider it necessary to carry out such an evaluation prior to
treatment activities.
11. If necessary, the person in charge will examine whether the treatment is in accordance with the evaluation
impact assessment relating to data protection, at least when there is a change in the
risk represented by treatment operations."
In development of paragraph 4, the Director of the AEPD approved a non-exhaustive list,
indicative of the types of treatment that require an impact assessment relative to the
data protection, indicating: "At the time of analyzing data processing, it will be
DPIA is necessary in most cases where such treatment meets

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

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

35.5 of the GDPR. The list is based on the criteria established by the “GUIDELINES

ABOUT THE IMPACT ASSESSMENT RELATED TO DATA PROTECTION

(EIPD) AND TO DETERMINE WHETHER THE TREATMENT "LIKELY INVOLVES A

HIGH RISK» FOR THE PURPOSES OF THE RGPD”, last revised and adopted on

4/10/2017, WP 248 rev.01 of WG 29 that complements them and should be understood as a

non-exhaustive list:

"4. Treatments that involve the use of special categories of data referred to

article 9.1 of the RGPD… or deduce information about people related to categories.

special data gories.

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

unique way to a natural person

.”

9. Data processing of vulnerable subjects…”

In the same Guidelines, it is stated:

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

DPIA due to its inherently high risk, taking into account the particular elements

Article 35, paragraph 1, and Article 35, paragraph 3, letters a) to c), the list that must

be adopted at national level pursuant to Article 35(4) and recitals 71, 75 and

91, and other GDPR references to processing operations that are “likely to enter

high risk", the following nine criteria should be considered:

"7. Data relating to vulnerable data subjects (recital 75): Processing of this type

of data represents a criterion due to the increase in the imbalance of power between the interests

parties and the data controller, which implies that people may be incapable of

You cease to authorize or deny the processing of your data, or to exercise your rights. Between the

Vulnerable stakeholders may include children (considered not capable of denying

gar or authorize knowingly and responsibly the processing of their data), employees"

The EIPD is a necessary step for data processing, not being as described,

the only one required is a budget to which the rest of the legal requirements must be added

for the treatment, legitimizing basis and respect for the fundamental principles of the treatment

Data processing provided for in article 5 of the RGPD.

Before implementing an RF system, the person in charge must assess whether there is another system

less intrusive with which the same purpose is obtained.

Biometric processing presents, among others, the following risks, some of which

contemplated in Opinion 3/2012 on the evolution of biometric technologies in the

GT 29 of 04/27/2012:

-The definition of the size (amount of information) of the biometric template is a matter

crucial. On the one hand, the size of the template must be large enough to handle the

security (avoiding overlaps between the different biometric data, or substitutions of

identity), and on the other, it should not be too large in order to avoid the risks of

reconstruction of biometric data

-Risks involved in the use of biometric data for identification purposes in

large centralized databases, given the potentially

harmful to affected persons.

-It goes without saying that any loss of the qualities of integrity, confidentiality and

availability with respect to databases would clearly be detrimental to any

future application based on the information contained in such databases, and would cause

also an irreparable damage to the interested parties. For example, if the recorded data of a

authorized person are associated with the identity of an unauthorized person, the latter

could access the services available to the owner of the data, without having the right to

it. The result would be identity theft, which (regardless of detection)

would make the system unreliable for future applications and, consequently, would limit its

freedom.

- The transfer of the information contained in the database.

-You can create the illusion that the identification through the face is always correct,

therefore, an analysis of the errors that may occur in its use must be included,

performance evaluation metrics, false acceptance rate- probability that a

biometric system incorrectly identifies an individual or fails to reject an individual

that does not belong to the group, and false rejection or false negative rate: the

correspondence between a person and his own template. Facing decisions that affect

legally to a person, any decision that is adopted based on it, as it could be

in registration and time control systems, the deduction of remuneration for registration with the

system, which should only be carried out while safeguarding the rights and freedoms and

legitimate interests of the interested party, at least the right to obtain human intervention

by the person in charge, to express their point of view and to challenge the decision.

-Linking: A large number of online services allow users to upload a

image to link it to the user's profile. The RF can be used to link the

profiles from different online services (via the profile picture), but also between
the world online and offline. It is not out of the realm of possibility to take a photograph of a
person on the street and determine their identity in real time by looking at these images of
public profile. Third party services may also track profile pictures and other
publicly available photographs to create large collections of images in order to
associate a real-world identity with such images. This impact increases with
increasing deployment of these technologies. Each individual may appear in one or several
biometric systems.

-Security measures must be adopted for the processing of biometric data
(storage, transmission, feature extraction and comparison, etc.) and about
especially if the person in charge of the treatment transmits that data through the Internet. The
security measures could include, for example, encrypting templates and
protection of encryption keys apart from access control and a protection that
make it virtually impossible to reconstruct the original data from the
templates. Additionally, use of realistic masks or use of photos to try
cheat the system, always in connection with the advances and the state of the art,
taking into account that the most effective biometric systems when it comes to recognizing a
person are also the most potentially vulnerable

Regarding the guarantees to be implemented that must be contained in the EIPD, the Guide “The
data protection in labor relations” of the AEPD contemplates, by way of reference
ten aspects that can be taken into account.

Likewise, the working document on biometrics, adopted on 08/01/2003 by WG29, considers
that biometric systems relating to physical characteristics that leave no trace (for
example the shape of the hand, but not fingerprints) or biometric systems

relating to physical characteristics that leave traces but do not depend on the memorization of data held by a person other than the data subject (in other words, the data is not stored in the access control device or in a central database) create fewer risks to the protection of the fundamental rights and freedoms of people (We can distinguish the biometric data that is processed centrally biometric reference data that is stored on a mobile device and the compliance process is performed on the card and not on the sensor or when the sensor is part of of the mobile device).

-It is generally accepted that the risk of reuse of biometric data obtained through from physical traces left by people inadvertently (for example: fingerprints digital) for incompatible purposes is relatively low if the data is not stored in centralized databases, but in the possession of the person and are inaccessible to third parties. Centralized storage of biometric data also increases the risk of using biometric data as a key to interconnect different databases, which could allow obtaining detailed profiles of a person's habits both at the public as private. Furthermore, the question of the compatibility of ends leads us to the interoperability of different systems that use biometrics. The normalization that requires interoperability can lead to greater interconnection between databases data.

The claim does not contemplate diverse and varied elements and scenarios that have been indicated in this section in its risk assessment, and has stated that it does not process data special character. However, the data is of that type, because when they identify unavoidably to the employee, since he has his template saved and when he presents the

sample, checks it among all the existing ones, fully identifying its holder to

through the samples that are saved on the device. As previously pointed out

processing of this type of data occurs.

In accordance with the available evidence, it is considered that the facts

posts do not comply with the provisions of article 35 of the RGPD, with the absence of any

type of documented impact analysis linked to facial recognition processing

from which the adoption of specific measures and guarantees derive.

viii

On the non-existence of guilt because he acted with the intention of protecting the health of his

staff, trying to guarantee the provision of essential services during the period

extraordinary confinement, and that is the first resolution by use of RF in the control

working hours, it must be indicated that guilt should be understood as personal judgment

of blame addressed to the perpetrator of a typical and unlawful act. This implies that the author

is the cause of the action that involves the unlawful conduct. that is attributable without the concurrence

circumstances that alter his capacity to act and that he is guilty, that is, that he has

acted conscientiously and voluntarily either intentionally or negligently.

It should be noted that the principle of culpability prevents the admission in administrative law

sanctioning objective liability, it is also true that the absence of

Intentionality is secondary since this type of infraction is normally committed

for a culpable or negligent action, which is sufficient to integrate the element

subjective of guilt. The field of simple non-observance is the classic of recklessness or

negligence, in its different degrees. From the material point of view, the guilt
consists of the ability of the obligated subject to act differently and, therefore,
Therefore, according to the legal system, within what is an interpretation
reasonable legal. Therefore, what is relevant is the diligence displayed in the action by the
subject, and what excludes the imposition of a sanction, solely based on the mere
result, that is to say to the principle of strict liability. In this sense, the Court
Supreme has understood that there is recklessness whenever a duty is neglected
legal care, when the offender does not behave with due diligence.
“However, the mode of attribution of responsibility to legal persons is not
corresponds to the forms of willful or reckless guilt that are attributable to the
human conduct. So, in the case of offenses committed by people
legal, although the element of guilt must concur, it is applied
necessarily differently from how it is done with respect to natural persons. According to
the S.TC. 246/1991: "(...) this different construction of the imputability of the authorship of the
infraction to the legal person arises from the very nature of legal fiction to which
these subjects respond. The volitional element in the strict sense is lacking in them, but not the
ability to break the rules to which they are subject. Capacity of infraction and, by
therefore, direct blame that derives from the legal right protected by the norm that is
infringes and the need for said protection to be truly effective and because of the risk that, in
consequently, must assume the legal entity that is subject to compliance with said
norm ". In this same line, the S.TS. pronounces on November 24, 2011 -appeal
258/2009-. “(Sentence 1456/2021 of the Supreme Court, third chamber, of the contentious
administrative, third section, of 12/13/2021, resource 6109/2020.
Regarding the concurrence of the pandemic, its interaction in the treatment of
data and its conjugation with the rights of the owners. The performance of essential services
cials does not imply the use of the facial recognition system that based on its prohibition

requires an analysis of its impact and the guarantees of the rights of its owners. On

which is a novel case, opinions and guidelines of the WG have been cited in this resolution

29 that involve interpretation of the rule, published on the web, dating back to: 2003,

2012, 2017, 2018 and 2020. Along with this, there are also reports on the matter from the AEPD

published on the web, elements that contribute to a reasonable and cautious interpretation

of the clear prohibition of data processing in the norm, in a system of evaluation of

risks and proactive, which does not record will carry out the claimed. Therefore, it follows that

if there is guilt on the part of the defendant when he could have acted differently

ink to which he did it, without the demand for exaggerated diligence.

IX

Article 83.4 RGPD states: "Infractions of the following provisions will be sanctioned-

shall, in accordance with paragraph 2, be subject to administrative fines of EUR 10,000,000 at most.

maximum or, in the case of a company, an amount equivalent to a maximum of 2% of the

global annual total business lumen of the previous financial year, opting for the ma-

higher amount:

The obligations of the person in charge and the person in charge under 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, it is considered

They are serious and will prescribe after two years the infractions that suppose a substantive violation.

of the articles mentioned therein and, in particular, the following:

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

treatment operations in the protection of personal data in the cases in which

that it be required."

X

Article 83.7 of the RGPD states that "Without prejudice to the corrective powers of the

supervisory authorities under Article 58(2), each Member State may

establish rules on whether and to what extent administrative fines can be imposed on

public authorities and bodies established in that Member State.

In this sense, article 77 of the LOPDGDD points out:

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

are responsible or in charge:

[…]"

d) Public bodies and public law entities linked to or dependent on

Public Administrations"

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 organic law, the

competent data protection authority will issue a resolution sanctioning

the same with warning. The resolution will also establish the measures that

appropriate to adopt so that the conduct ceases or the effects of the infraction are corrected.

would have committed

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

depends hierarchically, where appropriate, and those affected who had the status of

interested, if any.

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

It will also propose the initiation of disciplinary actions when there are indications

enough for it. In this case, the procedure and the sanctions to be applied will be the

established in the legislation on the disciplinary or sanctioning regime resulting from

app.

Likewise, when the infractions are attributable to authorities and managers, and it is proven

the existence of technical reports or recommendations for treatment that would not have

been duly attended to, the resolution in which the sanction is imposed will include

a reprimand with the name of the responsible position and the publication will be ordered in

the corresponding Official State or Autonomous Gazette.

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 the analogous institutions of the

autonomous communities the actions carried out and the resolutions issued under

of this article.

6. When the competent authority is the Spanish Agency for Data Protection, this

will publish on its website with due separation the resolutions referring to the

entities of section 1 of this article, with express indication of the identity of the

responsible or in charge of the treatment that had committed the infraction.

When the competence corresponds to a regional data protection authority,

It will be, in terms of the publicity of these resolutions, to what its regulations have

specific.

Article 26.1 of the RGU, states that: "the collaborating urban entities will have administrative nature and will depend in this order on the urban administration acting".

The defendant is an entity that has a legal-administrative nature for the fulfillment of its purposes, constituted in this case with a mandatory character by the will of its members, as reflected in the Statutes, which aims to preserve the urbanization works and maintenance of facilities and services by its grouped owners

Law 29/2001 of 1707, on land, of the Community of Madrid (BOCM of 07/27/2001, which has exclusive jurisdiction in matters of Urbanism in its article 137 indicates:

"Urban conservation entities":

"1. Urban planning conservation entities are entities governed by public law, mandatory affiliation and legal personality and capacity to comply with their ends.

2. They are governed by their statutes within the framework of this Law and its regulations and they acquire legal personality from their registration in the administrative register of the Ministry responsible for urban planning

."

The objective for which an urban conservation entity is constituted is to attribute to the owners of a certain urbanization the conservation of this, a function that initially it would correspond to the City Council or City Councils of the municipal terms in which the urbanization is framed. These entities receive both contributions from the owners who pay the corresponding fee as public funds. given this public nature qualified as a Public Law entity, dependent on the Ministry Environment, Housing and Agriculture, the regime established in article 77 of the LOPDGDD regarding the imposition of a warning sanction.

Therefore, no administrative fine would be imposed.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

39/40

the Director of the Spanish Data Protection Agency RESOLVES:

SANCTION with warning

URBAN DEVELOPMENT ENTITY

FIRST:

EUROVILLAS CONSERVATION COLLABORATOR, with NIF G79414033, for the

GDPR violations:

a

-article 9.2.b) of the RGPD, typified in article 83.5 a) of the RGPD and in 72.1. e) of the

LOPDGDD.

-article 35 of the RGPD, typified in article 83.4 a) of the RGPD and in 73.t) of the

LOPDGDD.

SECOND: NOTIFY this resolution to the URBAN ENTITY

EUROVILLAS CONSERVATION COLLABORATOR, with the sending of ANNEX

GENERAL and the DEPARTMENT OF THE ENVIRONMENT, HOUSING AND AGRICULTURE of the

Autonomous Communities of MADRID.

THIRD: COMMUNICATE this resolution to the Ombudsman, in accordance

with the provisions of article 77.5 of the LOPDGDD.

FOURTH: 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 period of one month from the day

following the notification of this resolution or directly contentious appeal

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

in accordance with the provisions of article 25 and section 5 of the fourth additional provision

of Law 29/1998, of July 13, regulating the Contentious-administrative Jurisdiction,

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

according to the provisions of article 46.1 of the aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP, it may be

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

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

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

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

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

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

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

effectiveness of the contentious-administrative appeal. If the Agency were not aware of the

filing of the contentious-administrative appeal within two months from the day

following the notification of this resolution, it would end the suspension

precautionary

Sea Spain Marti

C/ Jorge Juan, 6

28001 – Madrid

938-050522

www.aepd.es

Director of the Spanish Data Protection Agency

GENERAL ANNEX

Complainant: A.A.A.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es