 Procedure No.: PS/00010/2021

RESOLUTION OF PUNISHMENT PROCEDURE

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

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant) filed a claim on 11/25/2019 before the Spanish Agency for Data Protection. The claim is directed against DAVISER SERVICES, S.L. with NIF B43586809 (hereinafter, the claimed). The reasons on which he bases the claim are:

“The company has a file installed at the access door at the entrance of the warehouse industrial with fingerprint reading and operator code”.

“The company also has four more files installed at the access doors to the locker room, toilets and dining room also with fingerprint reading and operator password”.

Manifests:

-The fingerprint reader of the toilets fails very often since their hands are dirty by the working conditions motivated by the gloves they use and the dirt on the reader is accumulating. The sink for washing hands is accessed after signing in.

-Both employees of the staff and ETT of two more companies provide their services.

-Images are also taken with the video surveillance system that focuses on the door of the sink.

Provides:

-Copy of Labor and Social Security inspection report of 12/14/2018, in the center of work of the claimed, in order to verify the usefulness of digital markers and video surveillance cameras. In proven facts it appears:

On 11/13/2018 an employee could not access the services during her

day because the fingerprint marker that crosses the access to the

same. “In the presence of the inspector, an employee is required to access the

services and the worker is forced to repeat the operation several times to

get the door open.”

“Regarding the installation of digital scoreboards and security cameras,

surveillance, there is no formal communication to the legal representation of the

workers because it occurred prior to the first elections for

representatives of the workers in the company that were held in September

2017.”

The Inspector agreed to initiate sanctioning proceedings by means of an infraction act for

cause an employee a situation that violated her dignity and the employee is required to

2/31

company a modification of the service access system in order to avoid incidents

Similar.

The complainant states that the company issued a joint negotiation proposal in

June 2019, where it was indicated about the requirement of the Labor Inspection:

“the access buttons will be changed, and in addition, the installation will be carried out

with two buttons, one external and one internal to open the door in case of emergency”,

that ended "without any conformity", taking the company that unilateral decision to place

two extra buttons.

The complainant considers that the implementation of the footprint system is not ideal,

proportional, nor balanced and that the purpose and uses were not previously informed, as well as

of the exercise of rights.

SECOND: In view of the facts denounced in the claim and the documents

provided by the claimant, the General Subdirectorate for Data Inspection transfers the 3 and

02/17/2020 the claim to the claimed.

On 03/26/2020, the respondent stated:

1) The MPH company provides you with the "comprehensive schedule management service", parameterization and

technical support. Indicates that the biometric identification through the fingerprint consists

in the treatment solely and exclusively of a series of relevant coordinates obtained

of the fingerprints of the users that are processed and encrypted by means of a

algorithm, obtaining as a result a hash code known as "minutiae",

guaranteeing its irreversibility.

“The information described, as well as that obtained from the resulting treatment, is

duly registered and stored on the MPH servers installed at its headquarters in

Las Palmas de Gran Canaria, which in no case will allow the user or

interested applicant, manipulation or variation of registered data.”

It indicates that: “as established by Royal Legislative Decree 2/2015 of 10/23, which approves the

Consolidated text of the Law of the Workers' Statute, (ET) in its modification by the Royal

Decree Law 8/2019 of March 8/03, MPH in its capacity as treatment manager,

will keep the data generated for the provision of the comprehensive management service

schedules for 4 years.”

2) In 2014, the first attendance control system was installed only for

entrance and exit accesses of the ship.

“The purpose of these markers was to control presence and security in the

access to facilities.”

“About the new markers for access to facilities and services, in the

year 2017 a new system of markers is installed, the current one and in force, with new

markers for both the entrance to the ship's exit and for access to the services,

implementing a new data processing software in the cloud.”

“The purpose of the markers is the presence control, the security in the control

of access to the company's facilities, and to know the number of people who are

in the enclosure of the ship.

3/31

3) States that the implementation of the transfer system has not had the purpose of

control the time that a person is in the toilet, "the length of stay is not saved

in those dependencies", but "the purpose is that they access the "private

of the company: service, the locker room etc., only authorized personnel to prevent the

access to outside personnel, such as commercial carriers, etc.”

4) “The decision adopted after the claim is the maintenance of the transfer system.

-Provides three photographs under the title “photographic report of the manual call points”. In the

first, you see a digital marker (tab) and a black button. at the foot of the

photo puts "digital dialer for access to the facilities and emergency button for

get in ".

In the second photo, another digital marker and close to a red button located on its left

on some tiles. In the third photo, another digital scoreboard with the black button next to it.

right on the same type of tiles as the second photo, adding the label of these

last two: “digital exit markers to services and emergency buttons

to go out".

-Provide a copy of the treatment order contract with the MPH company, indicating in the

second clause that the data will be made available to the person in charge of the treatment

personal name and surname, national identity document, minutiae of the fingerprint,

data related to the job, department, category, shift, etc., email of the

user, signature / digital signature and, where appropriate, the code of the worker assigned to him, in

Otherwise, MPH will assign an alphanumeric code that will identify each user. I know

indicates that the entity is certified certified in the National Security Scheme and in

ISO 27001

The collection of the biometric data is carried out in the facilities of the person in charge of the

treatment and will be carried out through the hardware devices owned by the

treatment manager, who through remote access incorporates them into their data systems.

information located in the central facilities of the person in charge of the treatment.

- Provide a copy of the activity record of the person in charge of treatment, description of

data processing, indicating that it provides time control services through terminals

of signing that transmit to their central servers all the information to be treated already

that the client accesses through the web portal using a username and password.

Types of data managed in data processing, DNI, name and surname code

user/employee details of employment, number of days of absence including IT to

purposes of time control / time of presence fingerprint other biometric data the latter

It has the special category.

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

process the claim filed by the claimant on 06/9/2020.

FOURTH: Within the framework of the previous actions carried out by the Subdirectorate General

Data Inspection, in order to clarify the response of the respondent, dated

06/17/2020, you were asked:

1.

Impact evaluation.

He replied that they have not formalized the impact assessment on the implementation of the system.

signing procedure, given that the "in charge of the treatment carries out a treatment consisting of

a series of relevant coordinates obtained from the footprints, it does not use the entire footprint.

mind, but processes and encrypts them through an algorithm, obtaining the "minutiae", so

that it is not possible to know or establish the fingerprint of the person nor to know

who does it belong to.”

2. Number of workers of the entity where the control system has been installed

by fingerprint. Number of external people who come to the facilities.

He states that it is currently used in a workforce made up of an average of 30 people.

nas.

“There is no numerical control of external people outside the company who access,

because they are carriers who come for loading and unloading tasks, as well as auditing

third-party quality agents to control the product handled by the company.

sa.

An average of 4 or 5 visits per day could be encrypted, among carriers whose access is daily

and auditors whose access is very irregular.”

3. Information provided on the existence of a video surveillance area through photographs

of the poster or informative posters in which it is possible to appreciate both its location and the

displayed data.

Attach photographs in which you can see where each of the 4 cameras is placed

in the ship (one of them, states that it does not work, the 1) and identifies them with numbers. In the

Photo 1 shows camera 1 on the right, which is located on a yellow sign warning of

deosurveillance and camera two on the left. You can see 3 blue doors, the one on the right open.

ta that gives access to another space of the ship and the two on the left, closer to each other,

closed, and above them there is a clock on the wall. In these two closest gates between

yes, on the left there is a symbol of a sticker, toilet, or service.

Camera 1 focuses on the side and it can be seen that under camera two there are two doors

nearby blue and above them a clock on the wall on the door on the door.

Photo 2 is a broader view of these three doors, but you can see one more door than

seen in photo 1. This additional door (door four) is open, it is on the

left of the one with the toilet sticker symbol. Behind her is another closed door

(door five). In the antechamber of door five, you can see a recorder who has to his right

an access button. This recorder corresponds to the third photo of the "photo-report

graphic of the manual buttons", which reads as "digital output markers of the

services and emergency buttons to exit to the services and emergency buttons

agency to leave" that the respondent provided in the response of 03/26/2020 in the transfer phase.

do of the claim

On the door with the toilet sticker, to its left there is also a token and a button

access at the top left. This recorder corresponds to the first photo

of the photographic report of the manual call points, "digital marker for access to the

lations and emergency button to enter" that the respondent provided in the response of

03/26/2020 in the transfer phase of the claim.

5/31

On all doors on the floor is marked with yellow and black stripes

Provides images captured by the monitor on which the vision of each camera is projected, only

three images are seen. (chamber 2, 3 and 4).

The image identified as CAMERA 2 is seen on the monitor, obtained by the camera that is

located on a yellow informative video surveillance sign. The respondent identifies her as

CAMERA 1, which indicates "does not work", although the images are seen on the aforementioned monitor.

You can see the entire length of the side of the nave, incidentally, at the beginning is what

which may be the area of access to toilets, the floor has yellow and black stripes. Tea-

having the doors a recorder, anyone who accesses them can be identified

or go out

Close to the access door to the toilet and above it, there is another camera that shows

that focuses on the truck entrance area.

It states that "Cameras 3 and 4 focus directly on the warehouse and are poorly located,

so that if the warehouse is full of containers - as is currently the case -

there is no view of the warehouse.”

4. Explain the causes that have motivated the installation of the aforementioned cameras and what is the purpose of its installation.

The causes of the installation of the cameras are the control of the stock of the warehouse and the production, cameras 1, 3 and 4, and the view of the trucks entering the warehouse, camera 2.

5. Provide a copy of the communications sent to employees and their representatives to report the purpose of the installation of video surveillance cameras.

It states that the workers have “refused to sign the document on confidentiality and data treatment". The document it provides is a confidentiality agreement by ac-assign the user to data (in its functions it indicates that it has access to systems and supports in which contain information relating to personal data). Its eighth clause indicates that it treats your data for the management of the employment relationship. Nothing is contained about the camera system. Nor in annex 4, which is a compendium of the regulations of Data Protection.

6. Indicate the period of conservation of the registered images, together with the details of the measures taken to ensure that only authorized personnel access the recordings tions.

It states that the images are not kept, they can only be viewed live and access The monitor is performed only by the Administrator and Manager of the company.

FIFTH: On 02/19/2021, the Director of the AEPD agreed:

“INITIATE PUNISHMENT PROCEDURE against DAVISER SERVICIOS, S.L., with NIF B43586809, for the alleged infringement of article 5.1.c) of the RGPD in accordance with the established in article 83.5. a) of the RGPD.

For the purposes specified in the art. 64.2 b) of Law 39/2015, of 1/10, of the Procedure Common Administrative Law of Public Administrations, the sanction that may correspond

der would be a warning”

SIXTH: On 03/10/2021, the following allegations are presented by the respondent:

-Reiterates the answers given in the antecedents in the sense that “the informa-

The access control system does not store the fingerprint of the employees, but rather

minutiae are given and the system generates an algorithm that is not reversible and through which

the person cannot be identified.” There is no personal data.

-There is no access control system “of the people who access the toilets” or

Nor is access controlled to any other place in the company that is cited in the resolution.

tion but that the "access control system is limited to allowing access to those

users who are registered in the company system”, “without controlling or the person

nor the time that remains in that location” and “without storing any type of data of

personal character".

-The fingerprint access control system was technically suspended with

effects 04/01/2020, although it was partially reactivated from 06/01/2020 only that of access to

the ship and that "the access controls to the toilets are deactivated, the last being

record of use, the one made on 03/04/2020 and 03/05/2020.”

Attach a document signed by the Manager of the company that provides the management service.

tion and time control to the claimed, which indicates:

“The defendant has four contracted devices to record the day in their

facilities through the fingerprint, one located at the entrance that gives access to the center

work room and “three door-opening devices installed in their toilets”.

On 03/24/2020 they received from the client a request to suspend the contract due to the

COVID-19 pandemic”, “On 04/1/2020 the technical disqualification of the

installed devices and access to the contracted time portal software.”

“Dated 06/1/2020, the client received a request to reactivate the service, if

well it is verified that the devices located in the toilets received their last signing on

days 03/4 and 5/2020.”

SEVENTH: On 03/15/2021, it is agreed to start the test practice period.

He remembered:

1. Consider reproduced for evidentiary purposes the filed claim and its

documentation, the documents obtained and generated by the Inspection Services before

the defendant and the allegations to the initiation agreement PS/00010/2021 presented by the

claimed and the documentation that accompanies them.

2. In addition, the respondent is requested to respond or provide:

2.1- As stated in the file of your information

“The purpose of these markers was to control presence and security in the

access to facilities.”

“About the new markers for access to facilities and services, in the

year 2017 a new system of markers is installed, the current one and in force, with new

markers for both the entrance to the ship's exit and for access to the services,

implementing a new data processing software in the cloud.”

If the people to access the ship and in order to control labor presence-signing,

do they do it only with the fingerprint or does it have the addition of the introduction of a card? Case of

so be it, indicate what type of card, content and data stored.

If the same thing happens to access the toilets, or it happened until 03/05/2020.

Your response was received on 03/23/2021, stating that to access the ship in order to

of the time labor control only the footprint is used.

exterior toilets that give directly to the ship

It states that in the "

never any electronic access control.

Until 03/05/2020 and “for access to the changing rooms, by putting the fingerprint on the reader device

the access door to the locker room was opened only to registered users”.

” has not existed

2. 2- According to your information, the access system to toilets is different from the access system

by signing, since it intends for security reasons that only those authorized have access.

About this he is asked:

-Do all the employees of the entity coincide with the number of authorized persons, or are

do they have to add more people?

It states “that the employees of the company coincided with the number of authorized users

with access to the locker rooms and their internal services, and there were no authorized persons

external or external to the company with access to locker rooms.”

"External personnel or those outside the company access the external toilet by means of a key."

2.3-Copy of the printout of the latest toilet access records.

It provides a copy of the pdf file and indicates that: “from the months of February and March 2020 in the

which it can be verified that access to the exterior toilets was not recorded and that

security reasons only access to changing rooms was recorded

. “Since 03/05/2020, the

changing room access devices are deactivated, only the data of

entry and exit of the ship.

The provided file contains

“signing report”, 02/01 to 03/31/2020, counting and updating the accumulated hours

of each employee. 65 employees appear under the Personnel section, 4 in Logistics, 4 in J

Team, 3 managers and 1 Administration, total 76 without the Administrator. Reflects “mechanical output”

dico”, locker room entry or exit, each with a code, time of entry and exit, death,

family foundation, temporary disability to cite examples.

On it, it indicates that it is proven that accesses to toilets are not recorded, if sometimes

tuaries, only until 5/03/2020.

2.4-What is the difference between the footprint access system for the warehouse,

so to sinks, or what differentiated them until 03-5-2020? Indicate if they do not both work with the

previously recorded fingerprints.

It states that the “fingerprint reading device located at the entrance of the ship

records the time of entry of the time of departure of the ship in order to carry out the

time record.”

“Until March 5, 2020, the access door to the changing rooms and their toilets

interiors was closed, the fingerprint reader device that was located at the entrance

The locker room had the sole and exclusive function of opening the door for users.

registered users, it did not have time control functions”.

“at no time has any device been installed or access recorded

to the outside toilets.

2.5 Indicate what data is stored in the records of the toilets (according to the certificate).

There are three in charge of treatment, indicate in a sketch where they are found) to

that allow validation through the fingerprint, and what relationship do they have with the file templates?

Face-to-face exchange of entry-exit.

exterior toilets that give directly to the ship has never existed

-

He answers that in the

ca timers

.”

“The three locker room recorders, one at the entrance and two at the exit, do not store

data, they are simple readers that contrast the trace with the minutiae that the system has al-

stored in the cloud, if they match the system opens the door”

Additionally, you can provide any evidence that you consider that the access

with the fingerprint of the authorized employee, which corresponds to an employee of the company not

is identified as such when accessing the toilet, or the name of the person is not known

who accesses

It states that “at the accesses to the locker room, once the person is inside the locker room,

company does not know if you go there to drop off or pick up something from your locker or if

go to the locker room to use their indoor toilets.”

It does not provide sketches that allow visualizing the spaces, the recorders and the references that

locker room appointment, locker room recorder, lavatory: entrance lavatory recorder at each

of the two, and timer of departure of each one of them.

2.6 Briefly explain how the registration and storage system is produced.

tion of the fingerprint template, how it is formed and where the database is stored

of algorithms and what relationship it has with each recorder, connection, as well as the outgoing access

It gives the ship as a labor transfer and the spaces destined for access to toilets.

It states that to register a new worker in the system, the Personnel Manager

contact the person in charge of the treatment and it is this person who registers the operator in

the system by means of a code and who makes any modification in the transfers. This

company is the one that saves the data on its servers. The respondent cannot modify any

Some data on the signing of employees.

Provides contract with the person in charge of treatment dated 05/25/2018 already provided previously-

mind, and contract with the same entity of 03/19/2021 of "Comprehensive Management Service of

schedules” in which, among other services: “access will be facilitated to consult transfers,

management of requests, permits and licenses, through the Schedule Portal” to the client. accompanies

to the aforementioned contract as part of the same the "data and security lease contract

of information comprehensive schedule management service through the minutiae of the footprint.”

Figure information referring to different signing modalities including recognition

facial, telephone unit, signing to the mobile to give a few examples, not knowing which one has

been chosen.

Provide a copy of the activity record as the person in charge of treatment, indicating that they provide

time control services through clocking terminals that transmit to their servers

central all the information to be treated and to which the client accesses through the portal

Web with username and password.

2.7 In their allegations, in the certificate of the company that provides the service, it is indicated

that:

“The defendant has four contracted devices to record the day in their

facilities through the fingerprint, one located at the entrance that gives access to the center

work room and “three door-opening devices installed in their toilets”.

If it opens doors, does it mean that the fingerprint must be entered both when entering and when

exit?, and what difference exists in terms of the use and system of this modality with that of ac-

I go to the ship to sign?

It states that the company has contracted four devices

1 access to the ship

2 general locker room access

3 men's locker room exit

4 women's locker room exit

Indicates that only the ship access device has a clocking function for the

time check. The other three devices have door opener content and have no functionality.

time control purposes.

Since 03/06/2020, only the number 1 device is activated, which maintains

ne the clocking functions for time control.

It can be seen that it does not refer to any aspect of the recorders at the entrance to toilets placed

manifested in the Labor Inspection, although it does indicate the existence of two filers

of tread for the exit of the toilets.

EIGHTH: On 10/5/2021, a proposal for the literal is issued:

“That the Director of the Spanish Data Protection Agency change the sanction

from warning to administrative fine, for the infraction of DAVISER SERVICIOS,

S.L., with NIF B43586809, of article 5.1.c) of Regulation (EU) 2016/679 of the Parliament

European and Council of 04/27/2016 regarding the protection of natural persons in the

regarding the processing of personal data and the free circulation of these data (as far

hereafter, RGPD), in accordance with article 83.5 a) of the RGPD. That the fine, in

function of article 83.2. a), b) and g) of the RGPD and 76.2.b) of Organic Law 3/2018, of

10/31

5/12, Protection of Personal Data and guarantee of digital rights (hereinafter

LOPDGDD), is 20,000 euros.”

NINTH: On 10/20/2021, the respondent makes the following allegations:

1)

When resolving an initiation agreement for a sanction of warning and the proposal with

a sanction of an administrative fine of 20,000 euros violates the acts of the ad-

administration and violates the principle of legitimate trust.

Subsidiarily, it considers the sanction to be disproportionate for:

The fingerprint does not allow to identify the person. The data is not stored, it is not produced

affectation to any personal data, the data is not of the "essential in 2017" category.

The workers were duly informed and collaborated in the implementation. The end-

ity is the protection of workers. No harm has been done to workers

The company adopts measures when required by the Labor Inspection. Collaborate-

tion within the framework of this file.

2) The statement that the warning would not have a dissuasive nature lacks mo-

tivation.

3) The fingerprint system is habitual and adjusted to the law and respectful of the legal doctrine.

prudential in terms of access control to the facilities of the companies through

digital markers, considering that they do not have characters of illegitimate interference

in the sphere of intimacy.

In addition, in this case the worker is not identified nor is any sensitive data kept.

not even to be understood as such. They refer to the sentence they provide as

document 1, of the National High Court, appeal 774/2018 of 09/19/2019, grounds for de-

right v

Indicates that when the system was established in 2017, the biometric data had no category

special that the RGPD gives you. The regulations contained in the proposal cannot be applied

of resolution and consider that even the RGPD does not establish an absolute prohibition res-

regarding its collection and treatment, provided that it is adequate, relevant and not excessive.

It is related to the scope and the specific explicit and legitimate purposes for the

that have been obtained.

4)

It emphasizes that data processing in the strict sense does not take place, and therefore

workers' rights would not be violated, since it considers that the computer system

access control does not store the fingerprint of employees, but through

a series of random parameters or minutiae, the system generates an algorithm that is not

reversible and through or through which people cannot be identified only allow

You know that whoever accesses the changing rooms is not a person outside the company.

5) It is not possible to control the person who accesses the toilets, since the system is limited

to allow access to those users who are registered in the company's system.

sa, without controlling with it, the person or the time that remains in that location.

6) Regarding the proven facts, what is underlined is not correct, since it is either accre-

otherwise stated or the resolution is based on unverified instructor assumptions or

attacks against the documentary.

a.

(p. 9), this party has never indicated (nor has it been proven) that there are

sadors to enter and exit the toilet independently of the entrance to the locker room. I weighed

To this, throughout the resolution (ex. p. 12 of the same) this party is “accused” of not doing

cer mention “deliberately” the buttons to access the women's toilet. There is not

push-button system to access the toilets, neither female nor male, (there is no token-

additional room at the entrance to the locker room) there is only a push-button system to access the

two changing rooms, apart from the one that exists to access the ship”

Deductions that lack support, the resolution of the AEPD is transcribed and sub-

b.

underlines what has not been accredited, despite which the resolution considers it correct: (p.

10 Point 4)“…. According to what is deduced from the statements claimed in evidence, there is a

common access to changing rooms through the recorder who takes the fingerprint, and from the same in-

The interior can be accessed through different doors to male or female locker rooms. Consider-

realizing that to access the toilets there is a recorder, at least in the female one, in which

you enter with the taking of the fingerprint, to which the claimed person does not refer, the devices or record-

tors are according to the claimed:

1 Access and exit to the ship-to record the day of your employees-

employees in its facilities through the fingerprint, control purpose

schedule. It is recorded in the automated register-daily transfer report

of the company for each worker, time of entry and exit, total hours

shift and hourly balance.

2 For general access to the locker room (purpose of presence control, security

authority in the control of access to the company's facilities) is recorded

do also in the automated register - daily transfer reports - for each

worker, the time of entry and exit during the day-From the locker room

it is accessed by registering the fingerprint to toilets, although this recorder is not men

-

mentioned by the respondent. This access to toilets is not recorded in the

daily transfer report as such. To leave restrooms it is necessary to register

the footprint, ignoring whether it leaves from where you entered the locker room, or is an exit

independent of the entrance to the locker room, in which case it would be registering

in the daily transfer report this outing as time in the locker room. His end-

ity, according to the respondent, is the security that only authorized personnel have access

torized, although before accessing the toilet they would have already passed the

footprint when accessing the locker room.

c) (p. 11) of the resolution it is erroneously intended: "... The intended purpose

tends to only access toilets, authorized personnel, not external to the organization.

organization. The respondent offers information that is not very clear when stating that for

visits there is another area of toilets that would not coincide with the one itself when

that is accessed through the locker rooms, does not indicate how many locker rooms

there is, if there is only one entrance leading to two locker rooms, omit that you have

You will have to enter your fingerprint again to access the toilets, and you will be unlocked.

12/31

Noce if the lavatory exit is to another space other than the locker room. These

imprint issues in these spaces could be connected in this

case with the issue that employees have a break time

programmed during which is the time that they have to go to carry out their necessities.

needs, although in that case the purpose was not to control the obligations.

contractual reasons, but security of access to the installation, although it uses

employee data, so it mediates its use for a generic purpose

access security.”

d) (Page 12) erroneously establishes that “……. The respondent selected the

fingerprint registration for access to locker rooms and services. His end-

authority, control of authorized persons and for security, which have nothing

to do with the control and surveillance of the conditions of compliance with the

under derivatives of the contract, nor with the fulfillment of legal obligation im-

put on the businessman. These security reasons for access in a par-

of the facilities themselves, however, are reflected as a pro-

pia in the "hourly report" record of each employee's clocking, that is,

becomes part of the actual daily work record to be considered.

be considered as the time of making the worker available to the employer

sario and that is the object of what has to be recorded as a day.

The length of stay in toilets, or time of access-exit, according to claims

mado is not controlled, it is not his objective, although according to his explanation, he takes the

footprint, as they are inside the locker room that must be crossed with a footprint.

The issue is that the defendant also points out that he uses them as an open

doors, when in fact it is, through that activity, taking data

each time those spaces are accessed and left. nothing though

say of the additional recorder of entrance in toilets, the fingerprint is taken when

enter or leave the toilets. This access to toilets is not reflected in the interior.

schedule of each employee, which is included in the time of dressing

tuary, although the respondent does not give all the details of the registration recorder to

female toilet. Thus, regardless of the implication of the registry, each

data is processed every time toilets are accessed and exited, even if they are not captured

in the daily report or is it rather implicit in that record of time of

locker room, biometric data would be being processed for this purpose."

1) It refers to the documentary in the file and, in addition, accompanies as a document

ment 2 to 4, several photographs, which states "they were already in the file" for better

understanding and prove that the layout of the area has nothing to do with the one collected

the proposal. The photos did not appear in the file, since they were other shots in which no

it indicated by hand as now what each space is, nor was it seen from the front.

In the DAVISER 2 photo, you can see:

a.

Of the two doors below the clock hanging on the wall, and a third that could be seen

in the photos provided on the subject of video surveillance, that third door, wider,

located more to the right of the whole that when being open seemed to lead to another ship, it is

that of a "changing room, entrance and exit" according to the annotation in pen.

The narrowest door located to the right of the one with a sticker is according to

b.

the annotation in pen that sends on the photo, is the "lavabo people outside the company".

13/31

The widest door, located to the left of the door with the symbol sticker

c.

toilet is another "changing room, entrance exit" according to the annotation in pen.

In the DAVISER 3 photo, taken from inside a locker room, it can be seen that it has only

an entry and exit point, because it appears handwritten with a pen in the photo, fi-

marking the doors of two bathrooms inside the locker room, which do not have

they put a recorder, "bathrooms without fingerprint control" indicates the annotation, and it is not seen that

such a device exists.

In the photo DAVISER 4, taken from inside the other locker room, (different arrangement)

entry) it is seen that it has only one entry and exit point because it appears

handwritten with a pen in the photo, indicating the doors of two bathrooms in

its interior, which do not have a recorder, "bathrooms without fingerprint control" indicates the anomaly

tation, and no such device is seen to exist.

It should be noted that in tests a sketch with the spaces and clarification was already requested

of the spaces, and was not provided.

2) About the "document provided that reflects the length of stay of the workers-

in the locker room (and sink, showers, etc.)" states that "they do not compute for the purposes of working hours.

gives work ""For the purposes of the day, only the entry and exit button of the ship is computed."

3) Advocates against the proposal, that what is accredited is:

"A. There are two changing rooms: one for men and one for women. (document 2

to 4).

B. There is no common access to changing rooms through the recorder who takes the

footprint, and from the same interior you can access through different doors to

male or female locker rooms. There is evidence that there is

one door for the women's locker room and another for the men's locker room, and both, from

of the ship. (document 2 to 4).

C. There is no recorder to access the toilets, neither the female one, nor the mas-

culin (document 3 and 4), so it cannot be concluded as the instrument does

tructor, that as if there would be a signing system for the sink and therefore the

purposes of the recorder would be unrelated to security. The fingerprint must only be entered

drive to access the men's and women's locker room, not to access sen-

two sinks. Therefore, it has not been omitted by this part that the

footprint to access the sink as it is not.

D. The toilets are inside each locker room and you have only had to identify

the footprint when entering the locker room, not in the toilet. (document 3 and 4).

E. There is no recorder for access to the locker room for the purpose of controlling

presence, since it was proven that the day is controlled only with

the recorder of entry and exit of the ship.

F. It is said that it is ignored if you leave the bathroom where you entered the locker room,

or is it an exit independent of the entrance to the locker room, when the documentation

contribution provided, it was accredited that the entrance and exit of each locker room

is the same (document 2 to 4)

G. Between the access door to the men's and women's locker room, there are two

doors. One private and the other, which is the toilet of third parties outside the company

to which to access they must ask for a key (document 2). that there is a bathroom

specific for people outside the company, (which was proven to be

come to it) reinforces that the fingerprint identification system is

suitable, necessary and proportional and proves that the purpose of the system is not

other than preventing outsiders from entering the locker rooms of the employees.

two and responds to a security measure implemented by the company in be-

benefit of its employees.

H. Workers can go to the toilet and locker room when they need to

convenient, they have no predetermined time or fixed maximum time for

it. For the purposes of working hours, only the entry and exit button of the

ship. That is, if a worker enters the locker room and remains 8 hours

inside, this does not count for working hours since it would be recorded that he has worked

do from the entrance to the exit of the ship. This reality distorts that the finance

The functionality of the buttons for access to the locker room has the purpose of controlling

working day.

4)

It concludes that:

-Regarding the affirmation that is contained in the foundation of ter-

zero page 14 in that case the data processing takes place based on the

record of the fingerprint that allows to identify the employee who accesses the locker room

River, what was proven is that:

“The access control system does not control the person who accesses

1.

to the toilets, nor does it control access to any other place in the

company, but is limited to allowing access to those users who

are registered in the company's system, without thereby controlling the

person nor the time that remains in that location and without storing

any type of personal or identifiable data.”

The access control computer system does not store the fingerprint

two.

of working people, but through a series of steps

random parameters or “minutiae” the system generates an algorithm that is not

reversible and by or through which the person cannot be identified.

na. They only let you know that whoever accesses the changing rooms is not a person.

sound outside the company.

The previous points distort the last proven fact, number 7, to support

since no treatment activity is carried out.

- That the system does not affect privacy or imply any intrusion on the privacy.

employee privacy and is used to ensure employee safety.

employees confirm:

1. The necessary nature of the implemented system, as there is no other system

alternative, if the objectives (purpose) and the system itself are compared

respectful of the privacy of the workers, of whom we do not take

man data that violate any right.

2. The suitability of the system for the purpose for which it was implemented (protec-

ger workers from strange presences).

3. The proportionality of the system, especially when it does not entail prejudice or

inconvenience or disadvantage or violation of any fundamental right

for the workers.

It is the function of the company to guarantee the privacy of the employees, reason

whereby adopting a measure other than fingerprint identification,

could lead to the company being subject to complaints on the grounds

of the workers finding people outside the company in the locker room

company (a minimum of five).

PROVEN FACTS

1) The respondent stated in response to the transfer of the claim that he implemented in the

year 2017 a fingerprint collection and registration system. You have only one device

digital or recorder that serves for the entrance and exit of the ship where the personnel access

to work. "For access to services" installed another three digital scoreboards or

recorders, "implementing a new data processing software in the cloud." "The

purpose is that they access the "private company facilities: service, changing room

etc., only authorized personnel to prevent access to outside personnel, such as

commercial carriers etc.”

2) The respondent indicates that the implanted system consists of four devices that function

nan inserting the fingerprint of the employees (digital marker or recorders), registered

previously by the person in charge of processing the claimant who manages the “international service”.

schedule management manager. The activity of registering and managing the footprint is carried out

through a treatment manager contract dated 05/25/2018 with the company MHP

SERVICIOS DE CONTROL SL, for the provision of a comprehensive schedule management service through the minutiae of the footprint. Making available to the person in charge data of the companies employees, the person in charge registers the footprint of the employees of the claimed one that is processed and encrypted by an algorithm, being stored on servers owned by the processor.

gado. The record of treatment activity of the person in charge indicates that he provides services of time control through clocking terminals that transmit to their central servers all the information to be treated and to which the client accesses through the Web portal with username and password.

3) Of the photos provided in the resolution proposal by the claimed party, DAVI files-SER 2, 3 and 4, it is proven that there are two changing rooms -one male and one female- for the company personnel, with a digital dialer or common recorder to access, being necessary It is necessary to enter the employee's fingerprint. Inside each changing room there is a digital marker or recorder in which you have to enter the fingerprint to be able to leave. Do you see them-Tuaries according to the photos provided have lockers, benches. In each dressing room there are two

doors in which you access the toilet or the shower, being able to close. There isn't a digital marker or recorder for the access itself to this last space that comprises those two doors in each changing room, so the access and registration system It's to changing rooms/toilets. References to sink, internal services, which is made previously to the proposal should be understood as access to changing rooms/toilets for employees, located do on the ship. Access to sink is access to locker room/toilet. There is a toilet for visitors external that is none other than the one located next to the changing rooms, in a door that opens previous key request to the company

4) According to the respondent, about five visit the warehouse where its employees provide services. carriers every day, and occasionally product auditors. In tests, the claimed indicated that the company's employees coincided with the number of authorized users

with access to the locker rooms and its internal services, and "there were no authorized persons ex-

third parties or outside the company with access to changing rooms.” , and that “external or external personnel

the company accesses the external toilet by means of a key.” , sinks that are distinguished from the

internal parts of the ship, and that “at no time has any device been installed or

recorded access to outside toilets”.

5) The Labor Inspectorate agreed to initiate an infraction act on 12/14/2018 due to a complaint

of employees, verifying that “the digital scoreboard that opens the existing door to ac-

access to the women's toilet”, did not work properly, requiring the company to modify

cation of the system of access to services in order to avoid incidents against the dignity of

an employee. The defendant implanted, for the case of failure of the fingerprint to open toilets, a

button at the entrance and another one at the exit. Employees were also informed that “any

Any worker who needs to go to the toilet outside of scheduled break times

two, the team leader or the hierarchical superior present in the center will be notified” to

be able to replace the worker in the meantime. The act did not determine that the lavatories

previously yielded through the locker room and it was before accessing when you had to mark the hue-

there. Access to toilets should therefore be referred to as access to changing rooms/toilets as one,

one for the men's locker room/toilets, the other for the women's. is related to the statement

contained in the aforementioned infraction record (“the sink for washing hands is accessed

after punching, so it's obviously impossible to punch digitally with clean fingers.

peeps.”)

6) The devices, recorders or digital markers, are according to the claimed:

1 Access and exit to the warehouse (one)- to record the working day of its employees in

its facilities through the fingerprint, purpose of time control. It is noted

in the automated register - daily transfer report of the company - for each worker,

check-in and check-out time, total working hours and hourly balance.

2 For general access to the locker room (security purpose in the control of access to the

company facilities, which can only be accessed by those authorized, the personnel who provide services

claims for the claim) is also recorded in the automated registry-fi-report

Daily shifts- for each worker, the time of entry and exit during the day-To the dressing room-

both male and female river, it is accessed by registering the fingerprint in a digital marker or

common token, one. Inside the changing rooms that have lockers, benches and two

toilets, there are the toilets, two doors in each, which do not have another additional marker.

tional to enter. To leave the locker room you leave through the same place you entered,

for which, again, the fingerprint must be registered in a recorder located in each locker room

(total two recorders).

The defendant stated in evidence that the access system with a digital recorder for la-

bathrooms and changing rooms, understanding that they are not two different spaces, but changing rooms/toilets,

stopped working on the occasion of the declaration of the pandemic, on 03/05/2020.

7) According to the document requested from the person claimed in evidence: “signing report” of

the company, 02/01 to 03/31/2020, the number of workers amounts to 76. The fi-

chaje is updated, with the accumulated hours of each employee, and reflects aspects such as

“entry” or “exit” of the locker room, indicating the time at which he enters and when he leaves throughout

of the journey. The general rule is that the input is logged and the next is not logged.

entrance to the locker room/toilet as it could happen if it has to be used for the start of the

worked. The entrances and exits to or from the locker room/toilet do not occur or are related

with the times of entry or exit of the day. The respondent has stated in al-

tions to the proposal that ““For the purposes of the working day, only the entry button is computed and

departure of the ship."

FOUNDATIONS OF LAW

Yo

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

control, and according to the provisions of articles 47 and 48 of the LOPDGDD, the Director of the Agency The Spanish Data Protection Agency is competent to initiate and resolve this procedure.

ment.

II

Biometric data is defined by article 4.14 of the GDPR:

"biometric data": personal data obtained from technical processing

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

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

facial or fingerprint data;

It turns out that biometric data can always be considered as "information about

a natural person" since they affect data that provide, by their very nature, information

mation about a certain person. In the context of biometric identification, the

person is generally identifiable, because biometric data is used to identify

or authenticate/verify at least to the extent that the data subject is distinguished from any

want another.

In this sense, it is worth distinguishing the assumptions of biometric identification from the assumptions biometric verification or authentication. Identification is the process of recognizing a

particular individual among a group, comparing the data of the individual to be identified with

the data of each individual in the group (one-to-many). Verification or authentication is the

process of proving that the identity claimed by an individual is true, comparing the

data of the individual only with the data associated with their identity (one-to-one).

Biometric data have the peculiarity of being produced by the body itself and

definitely characterize. Therefore, they are unique, permanent in time and

person cannot be released from it, they cannot be changed in case of compromise-

loss or intrusion into the system.

A use is wide and without control of biometrics it is worrying from the point of

view of protecting the fundamental rights and freedoms of individuals. This type

of data is of a special nature since they have to do with the characteristics

behavioral and physiological characteristics of a person and can allow their identification

unequivocal

The apparent ease and innocuousness of collecting fingerprint data can cause

a false sense of security when it is precisely the opposite. Given the risks of

fingerprint reversibility, reconstruction from fingerprints found in

objects, increasingly frequent use of databases with interoperability of systems

fingerprint processing, false positives that would allow the admission or improper access of

your users who are actually not authorized, or false negatives when the system is not

admits an authorized sample, so it is necessary to establish principles and

specific guarantees in this regard

Regarding the alleged sentence, from the National High Court appeal 774/2018 of

09/19/2019, it is about the sanction that the AEPD imposed on the FITNESS MURCIA gym

PROMOTIONS SL, was issued before the entry into force of the RGPD. At the foundation of

Law IV indicates that the events "are from February 2017", "prior to the entry into

force of the RGPD" "which establishes a stricter regulation when biometric data is found

within the special categories of data."

It is convenient to determine the technical terminology used for an understanding of the matter, in

Regarding the references that occur in the context of the aforementioned judgment, of

example:

"Biometric information is stored in an algorithm."

"Minutia turned into algorithms".

"In effect, even if the fingerprint registration is transformed into an algorithm, the system

starts every time the member goes to the gym, putting his finger on

the digital reader which gives rise to the confrontation of data with the algorithm stored in

appellant systems.

"That is, originally the operation of the system is based on the reading of data

of the fingerprint that is introduced in a terminal and in the confrontation with the algorithm or se-

numerical sequence, which is incorporated, which is a permanent datum and which is in a

database of the appellant, which allows its association with the identity of the

Whoa. Therefore, based on unique data from each partner that is transformed into an algorithm and

that is verified at each entry, the data of the member who accesses the gym is being processed and

identification is allowed."

"Regarding the suitability of the measure, it should be noted that the collection and use of the fingerprint is

for the provision of a service, which is the access and use of the gym and that the registration

by means of a fingerprint obtains said identification/security that the person who

accesses the gym is what it claims to be when you put your finger on the reader and correlate your

registered algorithm, so that with it the intended objective is achieved and said judgment of

suitability is met."

"The appellant entity has been concerned about confidentiality with the conversion of the

fingerprint to its algorithm and have not kept the fingerprint or points of it in the system

but the algorithm

"the algorithm remains under the control of the user"

The AEPD has already made it clear in the published guide "14 misunderstandings in relation to

biometric identification and authentication" in its point 1: "the biometric information is stored

macena in an algorithm" "An algorithm (RAE) is a method, an ordered set of

operations or a prescription and not a means to store biometric data. Information

collected biometrics (for example, the image of a fingerprint) is processed following

procedures defined in standards and the result of that process is stored in re-

data records called signatures, patterns, template or "templates". These patterns

They numerically record the physical characteristics that allow people to be differentiated."

In addition, the guide values that the collection of biometric data can reveal data of the sub-

subject such as race or gender, emotional state, illness, substance use,

hello etc. , in an implicit way that the user cannot avoid as supplementary information

ria incorporated in its collection. The guide provides links to these claims that include studies

God scientists who conclude in these manifestations. That the identification processes

tion or authentication by biometric systems are not one hundred percent accurate as a system

password issue that is or is not the password. Biometric systems are based

san in coincidence or correspondence of probabilities, there are false positives, they give

For good an impersonation, or false negatives, it rejects an unauthorized individual. Nope

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

flexibility with respect to databases would clearly be detrimental to any application.

cation based on the information contained in said databases, and would also cause

irreparable damage to those concerned. For example, if a person's fingerprints

authorized were associated with the identity of an unauthorized person, the latter could

access the services available to the owner of the fingerprints, without having to

right to it. It raises a first question of proof on the part of the impersonated person who is

would face a technical system implemented by the person in charge, and that could lead to theft

which (regardless of its detection) would make fingerprints unreliable.

digital data of the person for future applications and, consequently, would limit their freedom.

Other risks as a case of suffering a security breach are that if the patterns of the

footprint are stored in more and more databases, it reaches more individuals, the reach

ce of the compromise of the data and your information to be restored is not the same as

if it occurred about the use of passwords.

The alleged sentence, due to the regulatory framework and the time it was issued, did not take into account

account the progress and knowledge of the risks inherent in this technology and above all

the exceptionality provided for by the RGPD, which on the other hand is a provision already issued in

2016, although with an entry into force deferred to 2018.

To perform biometric recognition, the biometric characteristics are transformed

through technical procedures on data in different formats: a sample (such as the

image of a fingerprint, a facial image) and a template (a reduced form of the

sample translated into codes, numbers). Biometric templates are stored.

The technical steps of biometric recognition can be reduced to:

The first stage of processing is the enrollment of biometric characteristics in a

biometric system. The biometric characteristics are "captured" in the form of a

image, such as a fingerprint image. The format resulting from this phase is called a sample.

biometric.

In a second stage, the information contained in a sample is extracted, reduced and transferred.

shaped into labels or numbers through an algorithm. This phase is called carbon extraction.

characteristics. Only "highlighted discriminatory information that is essential

for the recognition of the person. The extracted features are kept in a

biometric template in the form of a "mathematical representation of the biological characteristic

original metric. The template is a structured reduction of a biometric image: the

registered biometric measurement of a person. The created template contains the characteristics

personal of the captured parameters. What should be stored is the template, presented

digitalized form, and not the biometric element itself. The reference template

stores for comparison.

In a third phase, a biometric sample that is captured (such as a tip

finger) presented to a sensor with a pre-recorded template (such as the template

of a fingerprint).

Another point of great importance from the point of view of data protection is the
fact that some biometric systems are based on data such as fingerprints or
DNA samples, which can be collected without the interested party being aware, since
you can leave traces without realizing it. By applying a biometric algorithm to the fingerprints
digital keys found in a glass, you can find out if the person is registered in
a database containing biometric data, and in that case, determine your identity.
ity, by comparing the two templates. All this also happens with other systems.
biometric topics, such as those based on the analysis of keystrokes or the re-
distance facial knowledge, thanks to the characteristics of the technology used. The
problematic aspect is, on the one hand, that this collection and processing of data can
to be done without the knowledge of the interested party and, on the other, that regardless of their
current reliability, these biometric technologies lend themselves to widespread use across
because of its apparent innocuousness.
From these different technical stages and the transformation of the characteristics
biometrics on biometric information, various processing operations can be identified.
processing, as defined in article 4, paragraph 2, of the RGPD: in a first phase
(registration), data is collected; during the second phase (feature extraction),
data is organized, structured, adapted and stored; the final phase of the comparison
specifically involves the retrieval, consultation, use and disclosure of data.
III
From the outset, it is necessary to highlight the note of the restrictive character since, in principle, its
treatment is prohibited and can only be applied exceptionally, in
certain cases listed in the GDPR.
Article 9.1 of the RGPD starts from the same position, it indicates:
“Processing of special categories of personal data”

1. The processing of personal data that reveals ethnic origin is prohibited

or race, political opinions, religious or philosophical convictions, or

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

uniquely identify a natural person, data related to health or

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

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

following:

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

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

of the Union or of the Member States establishes that the aforementioned prohibition

in section 1 it cannot be lifted by the interested party;

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

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

of labor law and social security and protection, to the extent that

authorized by the law of the Union or of the Member States or a convention

in accordance with the law of the Member States that establishes guarantees

respect for fundamental rights and the interests of the

interested"

In this sense, recitals 51 and 52 of the RGPD make it clear: "Such data

should not be processed, unless processing is permitted in situations

specific provisions contemplated in this Regulation, taking into account that Member States

Members may establish specific provisions on data protection in order to

to adapt the application of the rules of this Regulation to comply with a

legal obligation or the fulfillment of a mission carried out in the public interest or in the exercise

of public powers conferred on the data controller. In addition to the requirements

specific to that treatment, the general principles and other rules of the

this Regulation, especially in what refers to the conditions of legality of the
treatment. Exceptions to the general prohibition of
treatment of those special categories of personal data, among other things when the
interested party gives his explicit consent or in the case of specific needs, in
particular when the treatment is carried out within the framework of legitimate activities by
certain associations or foundations whose objective is to allow the exercise of
fundamental liberties. (52) “Likewise, exceptions must be authorized to the prohibition of
treat special categories of personal data when established by the Law of the
Union or of the Member States and provided that the appropriate guarantees are given, in order to
protect personal data and other fundamental rights, when it is in the public interest,
in particular the processing of personal data in the field of labor law,
legislation on social protection, including pensions and for security purposes,
health surveillance and alert, the prevention or control of communicable diseases and other
serious health threats. (...)”

In this way, its treatment being prohibited in general, any exception to
said prohibition shall be subject to a restrictive interpretation.

The objective of the recognition through the fingerprint is that from the fingerprint placed
at the entrance terminal to changing rooms/toilets, find a series of points that coincide
with the stored patterns of the same fingerprint, in a set of stored patterns
in a database, all done in real time. Operation occurs at
basis of internally recognizing the trace that is presented to him in the recorder with the
registered in the database. The contrast is not made with the entire image of the
footprint that is not registered, but with the pattern of each person, which is unique and
contributes to recognition. Pattern extracted and stored in a database where
they store all the patterns of the requested personnel, that is, in a database

centralized. When the employee accesses the system showing in the recorder, bookmark digital or recognition module-there are several at the headquarters of the claimed, and for different uses or purposes-, his sample that he collects instantly, compares it, allowing the taking of decisions based on the degree of similarity obtained. Therefore, in this case, there is data processing, based on the registration of the fingerprint that allows the employee to be identified that accesses the changing rooms / toilets. Although there is no record of access to toilets, by accessing from the locker room, if it is considered necessary to assess that if you go to the toilet, to open the door of the locker room that leads to toilets, the obligation to enter such information when entering or leaving personal, permanent, invariable as the fingerprint with the risks that the use entails of said system. This, according to the respondent, to control that only the personnel access authorized, referring to people who do not belong to the company and could access these spaces. He has not offered further explanations on these security reasons, deducing on the other hand, that the toilet intended for these third parties, is located near the accesses to the changing rooms of the staff, but it is crossed with a key that facilitates the business.

In order to use this system, and for this specific purpose, in accordance with the parameters established in the GDPR, companies or organizations need to demonstrate high levels of proactive responsibility and design by default of Data Protection since before the treatment, including the fact of being able to justify first that there are causes for lift the prohibition of the treatment of article 9 of the RGPD in biometric data that in In this case, they would be based on security reasons in access to changing rooms/toilets.

IV

Regardless of whether the use of the footprint for access to changing rooms/toilets, the truth is that the fingerprint data is processed, and it is done on each occasion that it is accessed to perform daily physiological needs, and also, although it does not have a control purpose of presence, the truth is that it is reflected and forms part of the record of the day where

The entry and exit times are counted. True, it shares space with the

locker room that is first accessed, so that as stated by the claimed

You can go to this space for different reasons. Now, to this he adds that the time

spent in locker rooms/toilets:

- “They do not compute for the purposes of working hours. ““For the purposes of the working day, only the button

of entry and exit of the ship.”, adding

-"Workers can go to the toilet and locker room when they deem it convenient, not

They have no predetermined time and no maximum time set for it. For working hours only

23/31

computes the entry and exit button of the ship. That is, if a worker enters the

locker room and stays inside for 8 hours, this does not count for the purposes of the working day since

estuary that has worked from the entrance to the exit of the ship”

What it seems to indicate is that despite recording the time spent

for each employee in locker rooms/toilets, entry time, exit time, it is not necessary because

it is considered time worked, only the entry and exit counts, it does not interrupt the day. It

would presuppose that not only would the use of the system of

footprint for this purpose as analyzed in this case, but the constancy of said data does not

would be necessary. That record in attendance at locker rooms/toilets, each time it is accessed

and it leaves that space, registers the data and also treats it through the registration system.

other fingerprints for the purpose of security in access to them.

In the present case, it is considered that this system of access to changing rooms/toilets has

infringed article 5.1 c) of the RGPD, which indicates:

"1. The personal data will be:

c) adequate, pertinent and limited to what is necessary in relation to the purposes for which

are processed (“data minimization”)

Recital 39 also reiterates that obligation:

"…the specific purposes of the processing of personal data must be explicit and
legitimate, and must be determined at the time of collection. The personal data must
be adequate, relevant and limited to what is necessary for the purposes for which they are
treated. This requires, in particular, to ensure that its term is limited to a strict minimum.
conservation. Personal data should only be processed if the purpose of the processing is not
could reasonably be achieved by other means."

In the record of treatment activity of the person in charge, as well as in the contract of
treatment order did not figure that the print is going to be used at the same time as
access security measure, so that third parties do not access said spaces
reserved, or for access only by authorized personnel. This use implies a different basis
legitimizing.

In this case, it must also be assessed in the first place, that the system used is suitable
for the purpose, is necessary, and provided in its specific context, accrediting
that less intrusive technical measures do not exist or would not work.

This triple assessment requires exhaustiveness, starting, as has already been said, not only from
the prohibition of treatment of these data, since we are faced with categories
of personal data, but the risks of using intrusive technology, the
biases or the likelihood of misidentification, identity theft, and
type of unique identity that contains the fingerprint, the impact on the privacy of individuals,
the security measures and the proportionality or necessity of said treatment.

Given the growing interest in using these systems in different fields and, as they are
novel and highly intrusive identification systems for rights and freedoms
rights of natural persons, the constant concern of this authority of
control has been shared by the rest of the authorities for years, as they show
manifest:

-The working document on biometrics, adopted on 08/01/2003 by the Group of 29,

-Opinion 3/2012, on the evolution of biometric technologies, adopted on

04/27/2012, and that has led the community legislator to include these data among

the special categories of data in the RGPD.

This opinion indicates that: “When analyzing the proportionality of a biometric system

proposed, it is necessary to first consider whether the system is necessary to respond to the

identified need, that is, whether it is essential to satisfying that need, and not just the

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

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

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

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

-Opinion 2/2017 on data processing at work of the WG29 (adopted on

06/8/2017) establishes that "although the use of these technologies can be useful to detect or

prevent the loss of intellectual and material property of the company, improving the

worker productivity and protecting the personal data you handle

the controller, also poses significant challenges in terms of privacy and

Data Protection. Therefore, a reassessment of the balance between

the legitimate interest of the employer to protect his business and the reasonable expectation of

privacy of the interested parties: the workers”.

For this reason, "Regardless of the legal basis of said treatment, before its beginning,

must 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. This may be part of an assessment of

impact on data protection (EIPD)".

Before implementing a fingerprint identity recognition system,

the person in charge must first assess whether there is another less intrusive system with which

achieve the same purpose. Section 72 of CEPD Guide 3/2019 "on processing of

personal data through video devices", establishes in this sense that: "The use of biometric

data and in particular facial recognition entail heightened risks for data subjects' rights. It is

crucial that recourse to such technologies takes place with due respect to the principles of

lawfulness, necessity, proportionality and data minimization as set forth in the GDPR.

Whereas the use of these technologies can be perceived as particularly effective, controllers

should first of all assess the impact on fundamental rights and freedoms and consider less

intrusive means to achieve their legitimate purpose of the processing".

25/31

("The use of biometric data and, in particular, facial recognition entails

greater risks for the rights of the interested parties. It is essential that the use of

said technologies take place respecting the principles of legality, necessity,

proportionality and minimization of the data established in the RGPD. Whereas the

use of these technologies can be perceived as particularly effective, those responsible

should, first, assess the impact on fundamental rights and freedoms and

consider less intrusive means of achieving its legitimate goal of transformation.

The translation is from the AEPD).

Any business control measure such as this security in part of the facilities

internal that entails the processing of personal data, which affects their

holders, employees and employees, to be legitimate, must be analyzed from the triple judgment

of the:

-suitability: In this case, the defendant takes advantage of the use of the fingerprint in 2017 to implement it in order to "security in the control of access to the facilities of the business. Security in access to changing rooms/toilets through the footprint intended by the claimed can serve to prevent third parties from entering those spaces that, by not having registered the fingerprint will be prevented, despite the fact that it does not prove the problem of origin generated by visits, if they do, since they have their own space to use as sinks. A camera also captures images of the locker room door and of the visitors' toilet, which although it also captures another larger space of the nave, is it would recognize and the accesses would be seen. Neither is the use that of the aforementioned data can be expect according to GDPR.

-The need for treatment should not be confused with its usefulness. may be facilitate not having to know or remember the access code, carry a card, it is automatic and instant. Obviously a fingerprint recognition system can be useful, but it does not have to be objectively necessary (the latter being what really must be present). As established by WG29 - Opinion 3/2012 on the evolution of the biometric technologies - should be examined “whether it is essential to meet that need, and not just the most suitable or profitable”.

In this sense, the AEPD, analyzing the need for a treatment, concludes that, "If it is necessary or not, in the sense that there is no other more moderate measure for the achievement of such purpose with equal efficiency by being able to carry out manually the exercise. The term need should not be confused with useful but if the treatment is objectively necessary for the purpose” -by all, PS/00052/2020-.

Necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objectives pursued and whether it is less intrusive in comparison with other options to achieve the same goal. It is also a principle of data quality and a recurring condition in almost all legality requirements

of the treatment of personal data derived from the right of Data Protection. But

there is an objective need for the treatment, if it is not essential to satisfy that need, the

treatment is neither proportional nor lawful.

In this case, the causes, motives or circumstances of why in and from

2017 and the system has not been changed, it is considered necessary to maintain the security of

access to internal facilities and that has to be done with employee data and that

In addition, they are biometric data for the purpose of controlling access to changing rooms / toilets through

taking the fingerprint, affecting their rights and establishing more data collections

when they are simply exercising their access rights to spaces necessary for

the performance of their duties. Access restriction can be done with other

alternative means and is not and does not constitute an area considered to be of special security for

require the degree of identification offered by the fingerprint, which is therefore not essential for

exercise third-party access control in this case.

-Proportionality, a logical link between the measure and the objective pursued. Furthermore, so that

a measure complies with the principle of proportionality, the advantages resulting from the measure

should not be compensated for the disadvantages caused by the measure with respect to the exercise

cio of fundamental rights.

To carry out the valuation to which reference has just been made, the respondent

it reveals security reasons in the control of personnel in these spaces. Five

visits approximately every day, compared to 76 workers who have to use each occasion

They need to go to the sink to enter the locker rooms/toilets. The defendant already has a

access control to the ship, and as personnel outside the entity it is in that group in which

that they should be informed of the limitations, as well as establish a modality

control subsidiary to prevent access to areas that take into account and respect the

employee privacy.

The proportionality judgment leads to the adoption of the system, considering that it was
necessary, produced less interference in the law, so that there could be no
an equally effective system whose implementation would imply less interference in the
employee right. And it is at this point that it must again be brought up
everything that has been indicated in relation to the special nature of the data
biometrics confers the RGPD and that requires special attention not only to the
proportionality but to the data minimization itself; that is, the data is only
object of treatment as long as it is completely essential for the
fulfillment of the intended purpose.

It must be taken into account as a background to everything, that the places destined for rest or
recreation of workers or public employees, such as changing rooms, toilets,
canteens and the like have special consideration in terms of data protection,
not only in the installation inside of devices that allow the capture of personal data,
for example, video cameras, as they are direct measures of invasion of the privacy of the employers.
employed, being prohibited. To this end, it must be inferred that the placement of devices,
in this case involving the processing of biometric data, which control and can relate
access to these areas, represent an indirect measure of control of access to
many spaces, being able to relate, for example, the length of stay, or the group of
people who stay in them. As a general rule and given the prohibition of this
type of control, other means must be established so that access to them is only
produced by authorized personnel, which guarantees the privacy and the right of the personnel in
a proportional system that does not sacrifice fundamental rights.

In this case, in addition, the reasonable expectations of the owner of the data in time and in
the context of treatment needs to be carefully assessed. monitoring
systematic and continuous relationship of the movements of the employee by the employer
It undoubtedly affects the reasonable expectations of the owner of the data. The interpretation of

The concept of reasonable expectation should not only be based on the expectations of the owner of the
the data with respect to its person in charge, but rather to the decisive criterion of whether it can be
reasonably expect to be subject to monitoring in a specific situation. The
surveillance of such areas or monitoring is an intense intrusion on the rights of
subjects. The legitimate interest of the employer in these spaces, except for exceptions,
shall prevail over the rights of the employees. There is a limitation of

rights with the obligation to enter the fingerprint when entering or leaving changing rooms / toilets without
that the suitability, necessity and proportionality for it concur. There is no accreditation
of a legitimate purpose for the control of access to those spaces, nor are they derived from their
implementation more benefits or advantages for the general interest than harm to others
goods or values in conflict
In the case examined, the stamp-based signing system for changing rooms/toilets is not the
the only one with which the intended purpose can be achieved when there are alternatives, it does produce
repeated and unwarranted interference with the rights and freedoms of employees
continued.
The inappropriateness and disproportionality and non-relevance or adequacy of the system are proven
fingerprinting to access changing rooms / toilets with the implanted purpose of
security of access of people to said spaces, due to their insufficient motivation, and
In general, there are undoubtedly methods so that third parties outside the company do not
access those spaces less intrusive than fingerprinting on each and every occasion
that the employee go to said spaces for needs.
v
It is also observed that after the initial agreement, and the proposal, the
made through the tests and that with the same system takes advantage of the footprint for another
non-labour purpose, which violates the rights of employees in the repeated taking

of their data every time they need to go to the toilets, entrance and exit.

Faced with the proposal, the respondent affirms that there was evidence and it was stated in the evidence file that clearly outlined where the locker room spaces were, their relation to the toilets or where they entered and left. The documents you provide as photos in the proposal (DAVISER 2, 3 and 4) in which they are seen from the front and the interior locker rooms and the two interior lavatory doors in each locker room, did not work in the file, because they were other shots in which it was not indicated in any sense and less, to hand as he did in the proposal, which is each space nor was seen from the front.

In this sense, if there are provided photographs of markers, of doors that are they envision, but at no time until after the proposal does identification occur of these aspects, and the terms of reference, both of the Labor inspection, and of the the claim and the allegations of the respondent give rise to the mistake that the recorders are when accessing the toilet, and of course without knowing until that moment location and or entrance of any of the same, or of the one intended for visits. This means correcting some aspects related to the location, the division of the locker room/toilet spaces which does not essentially affect the imputation and commission of the offence, nor its nature.

Under the reason of security of access to an internal space, in reality, they are limiting the rights with the taking of fingerprints in each occasion, being registered their data. That means of accomplishing the goal of fingerprinting all employees is not justified because five people visit the ship daily, citing reasons of security that are not developed or related to the need for the use of the system of the fingerprinting. Also, the fact that the data is actually taken from 76 people, not 30 as stated by the respondent, not knowing the reason, adding to this the duration, since 2017 with the 2018 incident in which the Labor Inspectorate intervened increase in the reasons to take into account to modify the sanction of warning.

All these circumstances must be taken into account with a view to proportionality and

dissuasion of the imposition of the sanction. Considering the aforementioned elements, the corrective action by the Agency must take into account that in this case the dissuasive nature of the sanction with a warning, given that this subsequent analysis reached after the investigation, it is appreciated and accredited that the nature and seriousness of the expressed conduct is of greater importance than was taken into account in the agreement of beginning. All these elements suppose that the imposition of warning is varied by the administrative fine, in accordance with the provisions of article 58.2.i) of the RGPD:

“i) impose an administrative fine in accordance with article 83, in addition to or instead of the measures mentioned in this section, according to the circumstances of each case”

The reasons for the sanction change were detailed in the proposal, and the motivation appears exposed in it, without material defenselessness being deduced.

Article 83.5 of the RGPD indicates:

SAW

"5. Violations of the following provisions will be sanctioned, in accordance with section 2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of of a company, of an amount equivalent to a maximum of 4% of the turnover global annual total of the previous financial year, choosing the highest amount:

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

Determines article 72 of the LOPDGDD:

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

a) The processing of personal data violating the principles and guarantees established in Article 5 of Regulation (EU) 2016/679.”

7th

The fine imposed must be, in each individual case, effective, proportionate and

dissuasive, in accordance with the provisions of article 83.1 of the RGPD. In order to determine the

administrative fine to be imposed, the provisions of article 83, paragraph

2 of the GDPR, which states:

"two. Administrative fines will be imposed, depending on the circumstances of each case

individually, in addition to or as a substitute for the measures referred to in article 58,

section 2, letters a) to h) and j). When deciding to impose an administrative fine and its

amount in each individual case shall be duly taken into account:

a) the nature, seriousness and duration of the offence, taking into account the nature,

scope or purpose of the treatment operation in question as well as the number of

affected parties and the level of damages they have suffered;

29/31

b) intentionality or negligence in the infringement;

c) any measure taken by the person responsible or in charge of the treatment to alleviate the

damages suffered by the interested parties;

d) the degree of responsibility of the person in charge or of the person in charge of the treatment,

account of the technical or organizational measures they have applied under articles

25 and 32;

e) any previous infringement committed by the person in charge or the person in charge of the treatment;

f) the degree of cooperation with the supervisory authority in order to remedy the

infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the way in which the supervisory authority became aware of the infringement, in particular if

the controller or processor reported the violation and, if so, to what extent;

i) when the measures indicated in article 58, section 2, have been ordered

previously against the person in charge or the person in charge in question in relation to the same

matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or mechanisms of

certification approved in accordance with article 42, and

k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as

financial benefits obtained or losses avoided, directly or indirectly, through

through the infringement.

For its part, in relation to letter k) of article 83.2 of the RGPD, the LOPDGDD, in its

Article 76, “Sanctions and corrective measures”, establishes:

"1. The sanctions provided for in sections 4, 5 and 6 of article 83 of the Regulation (EU)

2016/679 will be applied taking into account the graduation criteria established in the

section 2 of the aforementioned article.

2. In accordance with the provisions of article 83.2.k) of Regulation (EU) 2016/679, also

may be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the performance of data processing

personal.

c) The profits obtained as a result of committing the offence.

d) The possibility that the conduct of the affected party could have induced the commission of the crime.

infringement.

e) The existence of a merger by absorption process subsequent to the commission of the

infringement, which cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

g) Have, when not mandatory, a data protection officer.

h) Submission by the person in charge or person in charge, on a voluntary basis, to

alternative conflict resolution mechanisms, in those cases in which

there are controversies between them and any interested party".

In accordance with the precepts transcribed, in order to set the amount of the sanction of a fine to impose in the present case for the infringement typified in article 83.5.a) of the RGPD, of which the defendant is held responsible, are considered concurrent as aggravating the following factors that reveal greater unlawfulness and/or culpability in the conduct of the reclaimed:

-The nature, seriousness and duration of the infraction, considering, especially the Effects that the treatment produces continuously in the privacy of the workers

affected, in number of 76, since 2017 (83.2.a RGPD).

-Although one cannot properly speak of intent, the claimant did not take into account additional elements of compliance and guarantee of rights, has focused its reasons in part that it did not process biometric data, and without precautions or measures, so The lack of diligence in the way of acting is considered clear and serious (83.2.b RGPD).

--Affecting some special data (83.2.g RGPD).

As a mitigating factor:

-The defendant is not an entity whose corporate purpose or related to it is the data processing in the usual way (76.2.b of the LOPDGDD).

Considering the exposed factors, the valuation that reaches the fine for the infraction is of 20,000 euros.

As an additional measure within article 58.2.d) of the RGPD, the one leading to stop processing fingerprint data to enter or exit locker rooms/toilets, although the re-claimed to have carried it out.

Therefore, in accordance with the applicable legislation and having assessed the graduation criteria of the sanctions whose existence has been proven,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE DAVISER SERVICIOS, S.L., with NIF B43586809, for a

violation of article 5.1.c) of the RGPD, in accordance with article 83.5 a) of the RGPD, and

for the purposes of prescription of the infraction in article 72.1.a) of the LOPDGDD, a

sanction of an administrative fine of 20,000 euros, in accordance with articles 83.2.a).

b), g and 76.2.b) of the LOPDGDD.

SECOND: NOTIFY this resolution to DAVISER SERVICIOS, S.L.

THIRD: Warn the sanctioned person that he must make the imposed sanction effective once

that this resolution is enforceable, in accordance with the provisions of art. 98.1.b)

of Law 39/2015, of 1/10, of the Common Administrative Procedure of the

Public Administrations (hereinafter LPACAP), within the voluntary payment period

established in art. 68 of the General Collection Regulations, approved by Royal

Decree 939/2005, of 07/29, in relation to art. 62 of Law 58/2003, of 12/17,

by entering, indicating the NIF of the sanctioned person and the number of the procedure that

appears at the top of this document, in the restricted account number ES00 0000

0000 0000 0000 0000, opened on behalf of the Spanish Data Protection Agency

in the banking entity CAIXABANK, S.A.. Otherwise, it will be processed

collection in executive period.

Received the notification and once executed, if the date of execution is between

on the 1st and 15th of each month, both inclusive, the deadline to make the voluntary payment

will be until the 20th day of the following month or immediately after, and if it is between

On the 16th and last day of each month, both inclusive, the payment term will be until the 5th of

second following business month or immediately following.

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

provisionally suspend the firm resolution in administrative proceedings if the interested party

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

In this case, the interested party must formally communicate this fact in writing addressed to

the Spanish Agency for Data Protection, presenting it through the Registry

Electronic Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through

any of the other records provided for in art. 16.4 of the aforementioned LPACAP. Also

must transfer to the Agency the documentation that accredits the effective filing of the

Sponsored links. 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

Director of the Spanish Data Protection Agency

938-26102021