 File No.: PS/00441/2021

RESOLUTION OF SANCTIONING PROCEDURE

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

the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant) on 06/04/2021, filed

claim before the Spanish Data Protection Agency directed against the

DEPARTMENT OF HEALTH OF THE COMMUNITY BOARD OF CASTILLA-LA

MANCHA with NIF S1911001D (hereinafter, the claimed party). The reasons on which it is based

the claim are as follows:

“On August 19, 2020, I filed a complaint with the Spanish Protection Agency

of Data that consisted of TWELVE Facts perfectly delimited and independent”. "He

September 24, 2020 I received notification only and exclusively referred to the Fact

TWELVE".

"Of the rest of the Facts until now I have not had knowledge."

SECOND: Retaking the resolution of the procedure for the claim of 08/19/2020,

It must be indicated that it is resolved inadmissible for processing on 09/24/2020, notified to the

claimant and there is no record that an appeal was filed against it.

The inadmissibility resolution, file E/07538/2020, indicated in the heading:

"Regarding the documentation that has been sent to this Agency referring to MUTUA

OF WORK ACCIDENTS SOCIAL SECURITY COLLABORATOR 72

SOLIMAT confirms, first of all, its receipt."

“The identification of infractions, due to violation of security measures or due to breach of the

duty of confidentiality, is generally linked to cases in which the documentation

with personal data would have been exposed outside the scope of protection implied by the

facilities where the data is processed or with the verification of the existence of a

observation of the data processed by third parties, not appreciating in the present

sufficient documentary evidence to allow the deduction of a breach of the duty of

confidentiality or that the technical and organizational measures applied by the person in charge of the

treatment are not appropriate to guarantee a level of security adequate to the

risk. However, if you have additional documents that can prove otherwise

you can file a new claim.”

There is also a registry entry of "refusal of telework requested by the

claimant on 02/15/2019”, among other reasons, because due to the nature of the services

provided, require the physical presence of the employee and others referred to in article 2.2 of the

Royal Decree 57/2012 of 12/08 which regulates the provision of services of the

public employees teleworking in the administration of the Board of Directors

Communities of Castilla la Mancha

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

THIRD: On 06/8/2021, an extension of the claim of the 4th of the same

month, indicating:

Add on what was already denounced on 08/19/2020:

On documents 3 and 8 (teleworking resolution of 06/25/2019 and summons at the headquarters of

Occupational Risk Prevention Service), they were delivered without signing, returning

the documents, and they were later delivered to him for his signature in the office of the Secretary

Provincial (SP) in the presence of employees, considering that their right to

confidentiality regarding your data.

As new facts, it reveals:

a)-Requests of any kind, vacations, private matters, teleworking are made

through the application "personal of each official" CHRONOS, and shows by

the email received from the SP on 08/07/2020, which concatenates another from a Head of

Section, that "this official "could have inquired into my application without my permission"

(document 13 and 14). It is an email from the Head of Section that tells the SP: “With

dated 08/04/2020, the claimant submits a permit application through CHRONOS

by teleworking for days 08/5 and 08/2020 ""Dated today 08/05 I am trying to

reject the aforementioned request but due to technical problems inherent to the platform

CHRONOS is turning out to be impossible for me”. It indicates that that day 5, "his correct signing was

in red color”, “which appear like this when they have been modified by hand”. In the document of

registration of the application 14 that it contributes, the time of entry and exit appears, together with the addition to

hand, “they are in red”. “In addition, they have unilaterally blocked my requests for

Telecommuting carried out through the application. Contribute from document 15 to 27,

screenshots of two days per week, from 09/25/2020 to 06/2/2021, considering

"They have accessed without my consent" the SP and a Head of Service. Point out that you have

granted teleworking since 06/30/2020 due to administrative silence, and "they are putting

obstacles”, “to date I am still not enjoying it”.

b)-"I have been recording until 03/13/2020 with the fingerprint biometric data, when

there are other less intrusive means of signing”. "I have not been asked for consent." "No

the use and purpose of time control has been reported" "and above all that it was going to be used with

sanctioning purposes as has been done with me”. Contributes in documents 5, 6 and 11 the story

that on various days of different months, he attended the doctor, and he has not been counted as

effective provision of work during the time of said assistance.

c)-Due to travel restrictions, when residing in another town, he had to

request a certificate by contacting the Secretary of the Delegate, who asked him to

prepare the certificate the ID and address. Indicates that the person who performs the functions

of the Secretary does not correspond to the position that said person has been assigned, which

is an administrative assistant, and has not found the change from one position to another, and "I have

doubts that she occupies the position of Secretary of the Delegate", "and could have accessed

fraudulently to my personal data".

d)-With the delivery of documents 51, 52, 54 and 56 I received four "instructions", two first and

Last of the DS Health Delegate (05/14/2021, 10/16/2020 and 01/4/2021 and 05/13/2021)

third of the SP, delivered by the SP, "covered by" the Secretary of the Delegate in the

first document, by two people in the second, and two others in the third, whose

names and positions designates, indicating that they are people who are not part of the Service

of planning, management and inspection "and among its functions is not the access to

any type of confidential information" on files related to the investigation.

The documents are an internal note, subject: "service order instruction" in which reference is made to

the restructuring communicated on 05/10/2021, all the members of the service in which

frame, they inform you of the composition of your section and functions and collaborators, and you will be

orders to promote the processing of the files under its charge and attaches the

instruction of 4/01/2021.

The second interior note reviews the claimant's tasks, indicating files in which

must give the corresponding procedures, in accordance with article 6 of law 40/2015 on

instructions and service orders, noting that non-compliance may lead to

disciplinary correction.

the rest are similar

e)-Breach of the duty of secrecy by sending ***POINT.1 on 11/4/2020 an email

e-mail without a blind copy that summons the staff of the Delegation to practice a

serological test of COVID 19, with the information that we had to go, including a

list of names and surnames of each of the workers, along with date and time,

provide a copy of document 53. The email indicates that "I am attaching the date and time of the appointment to

those people who, having requested a rapid COVID 19 test, did not yet have it assigned"

and each employee is indicated the day and time and location. It comprises 83 people and the aforementioned

Head of Section, appears related to "Personnel Section."

f)-Lack of legitimizing basis (art 6) to treat the data private telephone number, which is

was forced to provide based on the meteorological situation produced in January 2021,

"Filomena", when developing the remote service.

Provide a copy of an email sent to you by another employee on 01/10/2021. The email,

based on instruction 1/2021 of 01/9/2021 of the D.G. Public function motivated by

existing meteorological situation, (dictated by the competence attributed in the Decree

80/2019 of 07/16, which establishes the organic structure and powers of the

Ministry of Finance and Public Administrations), and "in view of the fact that the interested parties

are expressing their willingness to take advantage of the modality of provision of services not

face-to-face during the days of January 11 and 12, 2021 should be clarified given the

exceptionality of the situation as well as the pressing need that motivates it", and

interprets and establishes some conditions of said instruction. It indicates that those who

find themselves in the situations described by the instruction must, apart from requesting it,

"be available to the service, providing contact telephone number and answering email

corporate, and where appropriate VPN remote control connection"

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

Protection of Personal Data and guarantee of digital rights (hereinafter

LOPDGDD), on 06/29/2021, the defendant was notified of the literal:

"The claimant... states that until March 13, 2020 he has been signing with his

fingerprint without having previously been informed of the use and purpose of the treatment

that they would carry out with your personal data, these being subsequently used to

sanction him."

And it is requested:

"…You must analyze the claim, and send this Agency the following information:

1.- The legal basis of the treatment and, where appropriate, circumstance that lifts the prohibition

to treat special categories of data, according to article 9 of Regulation (EU)

2016/679 of the European Parliament and of the Council of 04/27/2016 regarding the protection of

natural persons with regard to the processing of personal data and the free

circulation of these data (hereinafter, GDPR)."

2.- The purpose of the treatment.

3.- The adequate guarantees implemented for the protection of rights and freedoms

of people.

4.- The categories of interested parties (workers, clients, users, etc.) and the information

provided to them on the processing of data.

5.- The Impact Assessment carried out or reasons why it has not been carried out (for

know the list of personal data processing that require an evaluation of

impact, as well as any other information related to impact assessments,

You can consult the "EIPD Management" tool at https://www.aepd.es/es/guias-y-

tools/tools/manage-eipd)

6.- The decision adopted regarding this claim.

7.- Report on the causes that have motivated the incidence that has originated the claim.

8.- Report on the measures adopted to prevent similar incidents from occurring, dates of implementation and controls carried out to verify its effectiveness.

9.- Any other that you consider relevant.

You must also provide the documentation that appears in Annex I of this document when the treatments refer to the assumptions that are contemplated in it.

ANNEX I

1) If the claim is related to the use of fingerprints, you must provide the following information:

- Precise description of the operation of the instrument used to capture the fingerprints.

- Criteria used for coding and storing the captured information (if biometric data is stored raw or if it is processed in such a way that it is only stores a biometric template).

- Reasons that justify the necessity and proportionality of the use of biometric data for the intended purpose.

- Measures taken to ensure that data reuse is not possible biometrics for another purpose."

Additionally, point 2 requests another type of information if the data were

treated with facial recognition techniques.

FIFTH: On 07/29/2021, a response was received stating:

1- Indicates the regulations that regulate the deduction of remuneration to employed personnel

public for the part of the workday not carried out, and which does not deduct

that is punitive in nature. This treatment is registered in the Register of Activities

of Treatment (RAT),

available at https://rat.castillalamancha.es/detalle/1006,

called personnel management of the Ministry of Health, and as a legal basis the law

4/2011 of 10/03 of public employment in Castilla la Mancha and Royal Legislative Decree

5/2015 of 10/30 approving the law of the basic Statute of public employees and the

Royal Legislative Decree 2/2015 of 10/23 approving the consolidated text of the

law of the basic Statute of workers. Its purpose is to manage the file of the

personnel assigned to the Ministry, civil servant, temporary and labor, time control or

staff presence.

Types of data: data related to administrative infractions, NIF, DNI, number of

Social Security, name and surname, address, telephone, signature, email, number

of personnel registration, footprint. Other data: personal, academic and

Professional financial and insurance economic employment details.

It states that the legal basis of the "time control treatment

6.1.b), 6.1.c), 6.1.e) and 9.2.b), of the GDPR.

" is based on articles

2-The General Secretary of Health provides ANNEX 1, of which the following stands out:

The Order of 09/07/2009 of the Ministry of Public Administrations and Justice on

work schedules and vacations of civil servants indicated the duration of the working day

work, the fixed hours of presence in the workplace, and their supervision. In his article

13 indicates that "all the centers and offices of the administration of the Junta de Comunidades

of Castilla la Mancha and its public bodies that have a staff of more than 15

People must equip themselves with the appropriate electronic or computer means for the

Control of staff hours. In any case, compliance with the

current regulations on the protection of personal data."

"In the DPS of ***LOCATION.1, from ***DATE.2 to ***DATE.1, the system of

time control employee has been signed by fingerprint verification. "

It alludes to the regulations in force at the time this modality of

treatment, Organic Law 15/1999, of 13/12 on the protection of personal data

(LOPD), which is understood to apply when the system is established, to the authorization for it

to article 6 of said law: "Consent will not be required when the personal data

personnel are collected for the exercise of the functions of the Administrations

public within the scope of their powers; when they refer to the parties to a contract or

pre-contract of a business, labor or administrative relationship and are necessary for its

maintenance or compliance…" .

By order of 12/5/2016, the Ministry of Finance and Public Administrations, exercising

its powers over the creation, modification and deletion of files with data of

personal nature of various Councils of the Board, determined the creation of the file

PERSONAL, Official Gazette of CLM of 12/19/2016 in which it appears mentioned, "for the

management of the Ministry's HR", in types of personal data it contains, figure

among others: "footprint".

With the entry into force of the GDPR, this file was transformed into a treatment that forms part of the RAT called: "Personnel Management of the Department of Health".

"Following the resolution of the General Directorate of Public Function, (DGFP) of *** DATE.3, which extends the extraordinary measures in relation to time control of the personnel (provide a copy), employees from ***DATE.1 can use the computer work to carry out the signing in an alternative way to the fingerprint control device digital, in accordance with the resolution of 05/10/2020 of the DGFP, which was published in the CHRONOS app."

The Resolution of 05/10/2020, of the DGFP, on organizational measures and prevention of occupational risks for the face-to-face reincorporation of personnel indicates in point 4-B-8:

"Regarding the use of biometric reading devices for signing, it is will continue with the measure established on 03/13/2020 that makes it possible to carry out the signing through CHRONOS through the computer of each user or user", although it is specified that "All of this, without prejudice to the specificities and specialties of the type of personnel and public services to be provided by each Ministry and Autonomous Organization".

3- A copy of the "report of the Provincial Delegation of the Ministry of Health in ***LOCATION.1 regarding the information given to public employees who take possession in the aforementioned DP on the use of personal data managed by the application staff time control computer" requested by the General Secretary of Health. The report is dated 07/27/2021. The following is indicated in ANNEX III:

"At the time (September 2016) they were posted on the different boards of the Delegation Provincial, in view of all the staff, informative posters of the new transfer system (through fingerprint), as well as the purpose of the data collected, the existence of a file for these purposes, and of all other information forecasts included in the regulations on data protection in force at that time.

SECOND.- That the records in the recording of the fingerprint of public employees

were always carried out by personnel assigned to the Personnel Section of the latter

Provincial Delegation (by the Head of Section in approximately 90% of cases),

who also reported the purpose of the data collected (control of compliance

of the days, control of the schedule and other regulations established in the Order of 09/07/2009,

of the Ministry of Public Administrations and Justice, on work schedules and

vacations of civil servants and concordant regulations established in the Agreement

Collective applicable at all times.

THIRD.- That during the aforementioned operation the circumstance arose that some

public employee refused to provide his fingerprint, a circumstance that was resolved

providing the employee with a code that he must enter in the biometric terminal. In this

In this case, the terminal collects the employee's code and the date and time of entry or exit.

3- The adequate guarantees for the protection of the rights and freedoms of the

interested parties, states that they are necessary to guarantee compliance with the

data protection principles included in article 5 of the GDPR. In the case of control

schedule is only used to verify the presence of the worker at his workplace

during the time established by the Administration. "As stated in the

ANNEX 1, in case of non-compliance with the schedule, the part may be reduced from the payroll

proportional to the time not worked".

The data collected is adequate, pertinent and limited to what is necessary for the purpose,

"in the time control, only the date and time of entry/exit and the identification of the

employee, this could be the fingerprint if the biometric terminal is used".

5- The treatment has implemented the security measures that guarantee that the data

personnel present the minimum security risks, all according to the ANALYSIS OF

RISKS of the "time control" treatment of the Ministry of Health, accompany as

copy of ANNEX IV, with the following characteristics:

a) Date 01/16/2021, “initial version”, approved by the “data protection officer”.

Tool used, "MANAGES", from the AEPD website, which is based on the response of

questions and that gives a result on the level of risk, acceptable or not.

In the RAT, the purpose is to manage the "HUMAN RESOURCES OF THE DEPARTMENT:

-Affected groups: employees

-Types of data: related to administrative infractions, NIF-DNI, name and surname,

address, telephone, signature, email, personnel registration number, fingerprint, others

data personal academic and professional characteristics, employment details

economic and financial and insurance.

-Computer applications: ACCESS MANAGER, FICHAR, CHRONOS, RENO and RENO

WEB

-Evaluation category National Security Scheme: average.

For all time control tasks, the application used is CHRONOS, which also

stores all the data in a SQL Server type database.

Data life cycle: Within four phases (1 data capture, 2 classification

storage, 3 use treatment, 4 assignment or transfer of data to a third party for its

treatment). It is indicated in the 1 "data capture" that the data to carry out the signing is

You can collect in the following ways:

By reading the fingerprint in the biometric terminal installed in the

□

building entrances. The footprint is collected, and the date and time of entry and exit.

By entering a code provided to the employee and that he must

□

enter into the biometric terminal. In this case, the employee's code is collected and the

date and time of entry and exit.

Through the computer of each public employee in the FICHAR application

□

CHRONOS

Identified risks: There is a box with "Threat/risk" on the left side and on its

right section, "Residual risk", with the result low, medium. Highlights:

□

“Unauthorized manipulation or modification of information”: under

□

“Impossibility of attributing to identified users all the actions that are

carried out in an information system”: low.

It ends by indicating that the result obtained is acceptable, "so when implanting

the recommendations made the risk would be low”.

It is indicated as a recommendation:

“Opt for 1:1 biometric verification or authentication systems, using the formula of

combine code plus footprint in all cases. In addition, it is recommended that systems

are based on the reading of the biometric data kept by the worker, for

example on a card.

5-In a separate document, ANNEX V, a document is provided without signature, date or person responsible for

the one indicated:

"Report on the necessity and proportionality of time control in the Ministry of Health",

indicating that the Data Protection labor guide published by the AEPD admits the use

of the fingerprint as a form of identification for the time control of workers,

as long as all the principles of the GDPR are complied with.

Suitability: The measure enables the proposed objective to be achieved.

The time control by means of a fingerprint system manages to control the time of

entry and exit of personnel, eliminating the possibility of identity theft of the

employee.

Necessity: "There is no other more moderate measure to achieve such

purpose with equal efficacy.

The time control of public employees is a lawful treatment by the

Ministry staff services.

When assessing the implementation of one of these solutions, it was decided to introduce the

fingerprint identification since it is a less impersonable form than the others. Whether

uses the fingerprint, it can only be the employee himself who accesses the

signing. It was decided after verifying the misuse that was being given to other systems such as

identification cards or codes.

Therefore, there is no other measure that would make it possible to achieve this objective with the same

efficiency level.

As a consequence of the pandemic, the personnel services have set up a

new application, FICHAR, so that employees can clock in on their computer at the

start or end your working day, being recommended by the personnel services

the use of this application.

Proportionality (the measure offers more benefits or advantages for the interest

general than damages to other goods or values of conflict).

In this case, it is necessary to weigh whether the benefits are greater than the harm that this measure

You have not only the right to Data Protection.

The use of the footprint is a more rational and fair measure, since it ensures the moment

in which the employee has entered and left his workplace. Furthermore, avoiding

possible non-compliance with schedules by an employee is important since it can give

place other colleagues who have to assume their work. Although the use

of the footprint supposes a more invasive treatment, the benefits of this system not only for

the employer but for the public interest outweigh the damages to this right. Besides,

The rest of the alternatives, the use of credentials, of codes, do not prevent the impersonation of the

employee identity.

6-The biometric terminal complies with the BioAPI specifications (ISO/IEC 19784 standard); The

Fingerprints are stored in a centralized database on SQL SERVER 11.

-"To collect fingerprints, access control terminals with sensors are used

biometrics of the brand NITGEN-Fingkey Access model SW101". "These terminals are

connect to a central server through the corporate network. The fingerprint is stored in a

bb.dd. centralized in SQL Server 11 and is assigned for each user to the terminal or

terminals from which you can sign, not being able to sign in any other".

-"Both the coding and the storage of the fingerprints are carried out by the

ACCESS MANAGER application which is the one that manages all data transactions

between the terminals and the centralized database and follows the BioAPI specifications

(ISO/IEC 19784 standard). The application is the one that is in charge of the encryption whose logic is

completely hidden from both the end user and the potential programmer. ACCESS MANAGER does not store users' fingerprints. The fingerprint is transformed into a code from an algorithm, and subsequently removed. Provide screenshot with image "maintenance of traces" of ACCESS MANAGER in which it states "it no longer exists no biometric data."

- On the measures adopted to guarantee that it is not possible to reuse the biometric data for another purpose, indicates that fingerprints are processed exclusively by the ACCESS MANAGER application, from which they can only be registered or deleted, in no case copy and much less alter. "The prints are stored in a bb.dd. centralized in SQL Server 11 with the same security measures as the Service of Database has for the rest of bb.dd., that is, it is part of the infrastructure certified (ENS and ISO 27001 Compliance). Fingerprint encryption is performed internally and, by following the BioAPI standard, technicians consider that it makes it difficult to fingerprint reuse in other systems than Nitgen".

7- Regarding the Impact Evaluation, it indicates that it is a treatment that comes from the previous regulations, the PERSONNEL file that the Department of Health had registered in the AEPD. It was created by the Order of 05/12/2016, of the Ministry of Finance and Public Administrations, of creation, modification and deletion of files with data of personal nature of several Councils of the Junta de Comunidades de Castilla-La Mancha. (DOCM No. 244 of 12/19/2016). "This treatment has not undergone any technological change nor functional that justifies the realization of this DPIA."

8-About the causes that have motivated the incidence that has originated the claim, it is

refer to ANNEX I

9-About the measures taken to prevent similar incidents from occurring, dates

of implementation and controls carried out to verify its effectiveness, indicates that in the

data processing for personnel management and time control, information will be included

in the CHRONOS app.

SIXTH: On 08/12/2021, in accordance with article 65 of the LOPDGDD, the

admitted for processing the claim presented by the claimant.

SEVENTH: On 04/04/2022, the Director of the AEPD agreed:

"START SANCTIONING PROCEDURE for the DEPARTMENT OF HEALTH OF THE BOARD

OF COMMUNITIES OF CASTILLA-LA MANCHA, with NIF S1911001D, for the alleged

violation of article 35 of the GDPR, in accordance with article 83.4.a) of the GDPR."

"For the purposes specified in the art. 64.2 b) of Law 39/2015, of 1/10, on Procedure

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

sanction that could correspond would be a warning, without prejudice to what results from

The instruction."

EIGHTH: On 04/21/2022, allegations are received, indicating:

1) It reiterates that at the time the system was put into operation, the

legitimacy is found in article 6.2 of the LOPD:

2) Article 35.1 of the GDPR whose violation is alleged provides that the EIPD is before the

treatment and the principle of legality entails the need for normative predetermination

of illegal conduct and its sanctions. The subsumption of conduct in the type

default is not discretionary power of the Administration.

"In the present case, we understand that in the sanctioning procedure initiated, it could be
be violating the principle of typicality, since the registration system of the working day
work, by means of a fingerprint, was launched prior to the application of the
GDPR, that is, under the validity of the repealed Organic Law 15/1999, of 13/12, of
Protection of Personal Data, for which reason point 1 of the article would not apply.
35 of the GDPR to initiate the sanctioning procedure for its violation, since this
would go against the provisions of article 25.1 of the Spanish Constitution, which provides:
"1. No one can be convicted or penalized for actions or omissions that at the time
if they occur, they do not constitute a crime, misdemeanor or administrative infraction, according to the legislation
current at that time."

3) The initiation agreement states that the EIPD applies to existing treatment operations
that are likely to pose a high risk to the rights and freedoms of individuals
physical and for which there has been a change in risks, taking into account the
nature, scope, context and purposes of the processing, and the respondent considers that
there is no change in the risks since its implementation, being a very
consolidated, “fully known and used by all Board staff”.

4) Indicates that despite understanding the above, an impact DPIA is going to be carried out with the
participation of the competent entities (regarding the information society and
coordination of electronic administration, framed in the Ministry of Finance and
Public administrations).

NINTH: On 11/8/2022, a test practice period begins, assuming
reproduced for evidentiary purposes the claim filed by the claimant and his
documentation, the documents obtained and generated during the admission phase to
processing of the claim, and the report of previous investigation actions that form

part of procedure E/07369/2021.

Likewise, it is considered reproduced for evidentiary purposes, the allegations to the start-up agreement

of the referenced disciplinary procedure, presented by the defendant, and the

accompanying documentation.

The defendant is requested to provide or report:

to)

In their risk assessment they indicate:

-"For time control, one of the forms of data capture is the introduction of a

code provided to the employee and that he must enter in the biometric terminal".

In this regard, you are requested to report if it exclusively works with this code

this type of access -does not require a fingerprint- and which employees have the option of

use it, from what date and until when.

- It is indicated as a recommendation:

"Opt for 1:1 biometric verification or authentication systems, using the formula

to combine code plus fingerprint in all cases. In addition, it is recommended that

systems are based on the reading of the biometric data kept by the person

worker, for example on a card."

On the same, reasons why they did not decide to use this modality.

b) If the time control with fingerprint was interrupted during the pandemic, and

What system are you currently using?

c)

If the entity uses the fingerprint control system for time control

from ***DATE.2, to ***DATE.1, dates from which it began to be used

by the claimant, and if its use ceased on 03/13/2020, reason, and if the claimant used

daily fingerprint system. Reasons for discontinuing use in

general fingerprint system for time control on ***DATE.1, or if optional. if so

outside, legal basis used and information provided to employees.

Responds on 12/7/2022, after having sent the resolution proposal on

2/12/2022

It states that "the Resolution of the General Directorate of Public Function, of

*** DATE.3, by which the extraordinary measures are extended in relation to the

time control of the staff of the Administration of the Board of Communities of

Castilla-La Mancha, ordered the extension until /07/2020 of the suspension of the

time control rules established in article 13 of the Order of 09/07/2009 before

cited (provided for by the Resolution of the General Directorate of the Public Function of

03/16/2020 during the validity of the state of alarm), as well as that from

*** DATE.1, the signing would be carried out (compulsorily) through the computer of each

user or user (because the CHRONOS corporate application allows this technique).

Likewise, in the aforementioned report it was mentioned that this resolution was subject to

adequate dissemination to all personnel through its electronic publication on the bulletin board

of the CHRONOS corporate application."

"Regarding this Provincial Delegation, during the aforementioned period

by the General Directorate of Public Function of suspension of the rules of control ho-

rary and mandatory signing through the computer (until 10-22-2021 as will be seen in the

next paragraph), the biometric terminal located at the entrance to the center was covered

with a sign indicating the prohibition of its use, under the aforementioned instructions

and of the service instruction of the Provincial Secretary specific in matters of Co-

vid19, of 05-12-2020, where the use of the fi-

fingerprint and that the staff must mark their entrances and exits using

your computer through the CHRONOS application." Declares that the attached

aforementioned specific service instruction on Covid19, but it is not provided.

Currently, under the protection of Instruction 4/2021, of 10/22 of the General Directorate of the

Public Function, on time control of public administration employee personnel

General of the Administration of the Junta de Comunidades de Castilla-La Mancha and its

Autonomous Organizations, as of 11/2/2021 the signing for the time control will be carried out

through the biometric reading devices available in each work center

low, without it being able to be done through the computer of each user (except

In the case of personnel authorized to provide services by tele-

job). It is stated that the aforementioned Instruction 4/2021 is attached, but it is not

contributed.

d)

In the report of the Provincial Health Delegation provided in the transfer of

the claim, they indicated when the measure of the use of the fingerprint was implemented to

time control:

"THIRD.- That during the aforementioned operation the circumstance arose that

some public employee refused to provide his fingerprint, a circumstance that

was solved by providing the employee with a code that he must enter in the

biometric terminal. In this case, the terminal collects the employee's code and the

date and time of entry or exit. “

He is asked if during the establishment of this system there was an alternative to

employees to use one or the other means, as justified and to how many

employees reached this modality and because it was not offered to everyone.

He responded that "at the time when the staff section of the Delegation

Provincial Ministry of Health in ***LOCATION.1 recording of

the fingerprint to all personnel, it is indicated to them, albeit verbally, that in case

failure of the biometric fingerprint marking system, they can carry out the marking at

by entering your ID number followed by a password

four digits, so all staff know that there is an alternative to marking

through fingerprint.

Only one employee has refused biometric registration by fingerprint and was

exclusively provided the aforementioned signing alternative, only said employee

public has exclusively enabled the signing by code, and all

public employees can use it as an alternative to doing it through

fingerprint.

and)

They stated on transfer that:

“To collect fingerprints, access control terminals with sensors are used.

biometrics of the brand NITGEN-Fingkey Access model SW101”

Indicate if this statement is correct or not, it would be the correct one that "for reading the

footprints…"

He responds that, "consulted the ICT service", "they have answered:""For the collection of the

fingerprints are used both access control terminals (Fingkey Access model

SW101) and, in some cases, desktop fingerprint collection devices

(Fingkey Hamster), both with Nitgen brand biometric sensors. terminals

access control systems are also used to read fingerprints."

f) They state in the risk analysis of the time control treatment that when

there are new public employees who are incorporated, various

possibilities, among which are included the reading of the fingerprint, or the introduction of a

code, or signing from the computer. You are asked if you are given a choice between any of

all three, and if the same thing happens with those who had chosen the fingerprint option or

they were forced to use it.

Indicates that it has already been answered previously and that dialing from the computer does not

it is allowed since Instruction 4/2021.

g) Role played by the Data Protection Delegation in the

establishment of the time control system through the fingerprint, in the changes

of the GDPR, and in the risk assessment document.

He replied that "This time control system was installed in 2016, when it has not yet

there was a Data Protection Officer"

"Regarding the risk assessment, as a consequence of the claim object of this

test practice period, the DPD recommended to the controller that a

EIPD" Provide a copy of an email dated 04/27/2022 in which the unit of

data protection staff of the Board are informed that it is necessary to carry out a

evaluation of the impact of the treatment of time control, associating personnel from the DG

Public Function and representatives of the Ministry of Health

h) Threshold value at which the software indicates that a match has occurred between the

two fingerprints that are compared, and what recommendation for this case does the

maker.

“The security level is established in the configuration of each terminal according to the

authentication method used in it:

• The security level for 1:1 authentication is between 1 and 9, and the default value

is 5.

• The security level for 1:N authentication is between 5 and 9, and the default value

is 8.

If the security level is too high, the authentication failure rate may

increase, and if the security level is too low, the read error rate may

increase."

Yo)

Indicate what happens if you do not recognize the fingerprint that is presented to you, and if you would store

that person's template.

It responds that: "If the fingerprint presented to the control terminal of the

access, the program shows an error message to the user, not producing the signing

correspondent. If the user template is understood as the mathematical translation of the

Image of the fingerprint made by the biometric reader, it is stored in the bb.dd.

centralized when it is collected in the user registration process and copied to

each of the access control terminals in which said user is going to carry out

their signings. The fingerprint readings that are carried out at the time of clocking are used to

compare with those stored in the terminal itself and, in case of

match, record the user's identification, as well as the date and time of access.

Users have the option of identifying themselves with their AccessManager Identifier (which

we match with your ID) before placing your finger for fingerprint recognition.

In this case, the terminal only compares the fingerprint recently read with the one stored for that

user in the terminal itself".

j) How do they guarantee that the biometric template extracted with the acquired software is

specified only for that person and is not used by other data controllers

of similar systems.

It responds that: "from the different Ministries, the users of the services of

staff, they do not have access to the templates. They can register fingerprints through the

application and in that process they can 'help' through the application that said collection

be as fine as possible, but in no case can they manipulate the print, much less

copy it. The templates are only accessible at the bb.dd level. And the traces that are read to the

when making the signing, they are not stored, they are only used to compare with the templates."

k) It is considered that when the fingerprint signing system is used, if you leave, you will

he has to mark the footprint, and if he returns that same day he has to mark it again. indicate

as the employee has to do to justify the various reasons for which he can be

absent from work, providing the instruction or regulation that would have been made known to them.

It answers that "The reasons are implemented in CHRONOS, that is, you have to request in

the tool the situation that proceeds in each case and there is a list of

reasons for absence from job (registration of application, concepts) Also that

supporting documents are attached by CHRONOS."

l)

Inform if with the change of the RGPD information was provided to the

employees about the new elements of transparency in the processing of their data.

“No, at the time of the entry into force of the GDPR, but as a consequence of the complaint, the DPD recommended that the information from article 13 be incorporated corresponding to the treatment in the CHRONOS time control application of the Department of Health",

m) If they have already carried out the impact assessment stated in their allegations, a copy of it or the state in which it is found.

The DPD together with the Data Protection Unit recommended to the person in charge the carrying out an EIPD, not only of the treatment of time control, but of all the processing related to personnel management; therefore, the scope of the EIPD includes all those treatments in which there are two controllers, the General Secretariat of the Ministry of Health and the General Directorate of Public Function.

It is recommended that this be done since, according to what is stipulated in the decrees of competences, the Secretaries have the competence for the "superior leadership and inspection of the personnel of the central and provincial services" and the General Directorate of Function Public for "the elaboration of the regulations and instructions in matters of public function, legal advice and issuance of reports within the scope of its powers and the advice on human resources, as well as collaboration, assistance and coordination of bodies with competencies in personnel matters.”

“carrying out the evaluation in this way could be extrapolated to the rest of the Ministries of the regional Administration with the adjustments that, if necessary, should be made in the event of processing differently from any of the processes.” Provide meeting message

05/12/2022, indicating that the description of the data life cycle has been carried out, if

Well, the meetings are not held electronically, but by email.

SEVENTH: On 12/2/2022, the resolution proposal is issued with the literal:

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

warning to the DEPARTMENT OF HEALTH OF THE BOARD OF COMMUNITIES OF

CASTILLA-LA MANCHA, with NIF S1911001D, for a violation of article 35 of the GDPR,

in accordance with article 83.4 a) of the GDPR, and for the purposes of prescription in article

73.t) of the LOPDGDD."

EIGHTH: On 12/5/2022, the defendant agreed to the notification. With date

12/20/2022, allegations are received in which it indicates:

It reiterates what has already been stated and requests that the responses given to

1)

tests.

2)

Estimates that the control system with the fingerprint is proportional since it is not

has found no system that allows the same efficiency to meet the objective

to control the working hours of the public employee, since this is the only one who

forces the worker to travel to the workplace. Other systems, such as cards,

codes or the signature, do not guarantee that it is the worker himself who signs. They do not have

other systems such as computer transfers are equally effective, since the

worker, as has been verified in different audits carried out, can clock in from

other devices such as the home computer, mobile phone, etc., and therefore does not comply with the

purpose of checking that the worker is actually at his job.

On the other hand, the transfer system through the computer is not extensible to the entire

personnel, since there are public employees who do not have a computer. Also I know

they received many complaints from the staff about the time they lost since they entered

to the building, went to his personal computer, entered the program and signed. For all

For this reason, the computerized signing system is still maintained today

only for staff who telework on the days they do so.

Provide a copy of Instruction 4/2021, of 10/22 of the General Directorate of the

3)

Public Function, on time control of public employee personnel of the Administration.

General of the Administration of the Junta de Comunidades de Castilla-La Mancha and its

OOAA, in which stands out:

"First. As of November 2, 2021, the signing for the time control will be carried out

through the biometric reading devices available in each work center, without

that can be done through the computer of each user or user. Second. He

personnel authorized to provide services through teleworking will continue

recording the working time of each day carried out under said modality through

of the Chronos application, in accordance with section 4.3 of Instruction 3/2021, of 21

June, of this General Directorate of Public Function."

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

documentation in the file, the following have been accredited:

PROVEN FACTS

1- At the Provincial Health Office of ***LOCATION.1, (DPS) from ***DATE.2

until 03/13/2020, when the time control system is suspended due to the pandemic

employee has been signed by fingerprint verification. Since 03/13/2020,

the staff could clock in through each user's computer with an application

named CHRONOS. The claimant who provided services at said headquarters stated that

has been clocking in until 03/13/2020 with that system, applicable according to the claim for

official, temporary or labor personnel.

2- The Order of 09/07/2009 of the Ministry of Public Administrations and Justice on

work schedules and vacations of civil servants regulates the duration of the working day

work, the schedule, and the "need to provide electronic or computerized means

suitable for the control of staff hours, complying with current regulations on

Personal data protection."

Order 34/2020, of 03/15, of the Ministry of Finance and Public Administrations, by

which regulates the provision of services in the General Administration of the Board of

Communities of Castilla-La Mancha in development of the measures adopted as

consequence of the declaration of the state of alarm for the management of the crisis situation

health caused by COVID-19 established as a habitual mode of provision of

services, the remote modality, without prejudice to the fact that at any time they can

Face-to-face modalities may be required when necessary. In developing it, the

DG Public Function adopted extraordinary measures in relation to the time control of the

staff of the Administration of the CLM Communities Board, resolving to “suspend the

time control rules provided for in article 13 of the Order of the Admin Council.

Public of 09/07/2009 on work schedules and vacations of civil servants

The resolution of the General Directorate of Public Function on organizational measures and

prevention of occupational risks for the face-to-face reincorporation of

05/10/2020 stated "Regarding the use of biometric reading devices for

the signing, the measure established on 03/13/2020 that makes it possible to carry out the transfer will continue.

signing through CHRONOS through the computer of each user or user.”

3-As stated by the defendant, in the DPS of ***LOCATION.1, from ***DATE.2,

Until 03/13/2020, the time control system used has been the signing by

fingerprint verification, interrupted by the pandemic and resuming the

11/2/2021.

There is also a teleworking regime (only jobs that can be

teleworking) that is combined with face-to-face sessions-at least two a week

(Instruction 3/2021 of 06/29 of the DGFP) in which the registration of the day is made at

through the CHRONOS app.

However, in the risk analysis provided by the defendant, of 01/16/2021: as soon as

to the signing, indicates that the: "data capture" for the signing, can be collected from the

following forms,

 By reading the fingerprint in the biometric terminal installed in the entrances

triads of buildings. The footprint is collected, and the date and time of entry and exit.

 By entering a code provided to the employee and that he must enter

cir in the biometric terminal. In this case, the employee's code and the date and

check-in and check-out time." The defendant points out that there is only one employee to whom it applies

this system, which refused to provide the print, although it was verbally informed of this

option to all, circumstance that is not accredited.

Through the computer of each public employee in the FICHAR CHRO application.

NOS.- without specifying the temporary parentheses and the teleworking group:

4-By order of 12/5/2016, the Ministry of Finance and Public Administrations,

exercising its powers over the creation, modification and deletion of files with personal data of various Councils of the Board, determined the creation of the PERSONAL file, Official Gazette of CLM of 12/19/2016, "for the management of HR of the Ministry", in types of personal data it contains, among others: "footprint", in description -types of personal data it contains-, figure: "Data relating to infractions Administrative", with the General Secretary of the Ministry of Health as responsible.

The defendant states that with the entry into force of the GDPR, it became a treatment that is part of the Record of Treatment Activity, such as "management of Ministry of Health personnel", with the purpose: personnel file management official, eventual and labor attached to the Ministry, time control or presence of the staff, and as a legal basis: Law 4/2011 of 10/03 on public employment in Castilla la Mancha, Royal Legislative Decree 5/2015 of 10/30, which approves the law of Basic Statute of the public employee and Royal Legislative Decree 2/2015 of 23/10 by the that the consolidated text of the law of the basic Statute of workers is approved. In Types of data: "data related to administrative infractions, NIF, DNI, number of Social Security, name and surname, address, telephone, signature, email, number of personnel registration, footprint. Other data: personal, academic and professional employment details economic financial and insurance"

However, the defendant stated that the legal basis is based on articles 6.1.b), 6.1.c), 6.1.e) and 9.2.b), of the GDPR, and given that the measure was implemented before the entry into force of the RGPD, article 6.2 of the LOPD 15/1999.

5-As an extension of extraordinary measures with the time control of the staff of the Administration of the Junta de Comunidades de Castilla la Mancha, the D. General of the Function Public resolved on ***DATE.3, that the staff, from ***DATE.1 can use the

work computer to carry out the clocking alternatively to the control device

of footprint.

6- Fingerprints are stored in a centralized database in SQL Server 11, including

in the certified infrastructure. Control terminals are used to read fingerprints.

access with biometric sensors, brand NITGEN-Fingkey Access model SW101.

“These terminals connect to a central server through the corporate network. The footprint

is stored in a centralized database in SQL Server 11 and allocated for each

user to the terminal or terminals from which they can clock in, not being able to clock in any

other". The ACCESS MANAGER application transforms the fingerprint into a code through

based on an algorithm, and manages all data transactions between the terminals and the

centralized database, also the collection or registration of the fingerprint and encoding,

the fingerprint code is stored in encrypted form, which fingerprint is then eliminated.

7- Through the fingerprint used by the defendant, and that serves the purpose of

time control, at the entrance and exit of the work center, the defendant makes a deduction of

assets, adjusting in its calculation to Law 1/2021 of 02/21 on complementary measures

for the application of the plan of guarantees of social services of the CCAA of Castilla la Man-

cha, BOE 08/13/2012. The defendant performs the time control tasks using a

application called FICHAR CHRONOS, which also stores all the data in a

SQL Server type database, and in which employees clock in on the computer (RAT),

from 03/13/2020, as a consequence of the pandemic, at the beginning or end of your day

employment, "without prejudice to the specificities and specialties of the type of personnel and

public services to be provided by each Ministry and Autonomous Organization”

8- The defendant carried out a risk analysis on 01/16/2021 with the tool

MANAGES (which the AEPD puts on the web), based on a sheet to complete with

answers 17, giving a result of:

-Identified risks: There is a box with "Threat/risk" on the left side and on its

right section, "Residual risk", with the result low, medium. Highlights:

 “Unauthorized manipulation or modification of information”: under

 “Impossibility of attributing to identified users all the actions carried out

carried out in an information system”: low.

It ends by indicating that the result obtained is acceptable, "so when implanting

the recommendations made the risk would be low”.

It is indicated as a recommendation:

“Opt for 1:1 biometric verification or authentication systems, using the formula of

combine code plus footprint in all cases. In addition, it is recommended that systems

are based on the reading of the biometric data kept by the worker, for

example on a card.

9-According to the defendant, the adequate guarantees for the protection of the rights and

freedoms of the interested parties are those related to compliance with the principles of

data protection included in article 5 of the GDPR. In the case of time control only

It is used to verify the presence of the worker in his place of work during the

time set by the Administration. “As indicated in ANNEX 1, in

In the event of non-compliance with the schedule, the proportional part of the payroll may be reduced

time not worked”.

10- In a different document, without date or signature, referring to the suitability, necessity and pro-

proportionality refers to the claim to its use to avoid impersonating the identity of the employee, and

that the footprint was decided "after verifying the misuse that was being given to other systems

such as identification cards or codes” without providing probative evidence.

11-Regarding the Impact Assessment, the defendant indicates that she is not obliged to carry it out,

because it is a treatment that comes from the previous regulations to the RGPD. Indicates that

"This treatment has not undergone any technological or functional change that justifies the

completion of this DPIA.”

12-In evidence, the defendant answered that she was preparing an impact assessment of the

time control.

FUNDAMENTALS OF LAW

Yo

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter GDPR), grants each

control authority and as established in articles 47, 48.1, 64.2 and 68.1 of the Law

Organic 3/2018, of 12/5, Protection of Personal Data and guarantee of rights

(hereinafter, LOPDGDD), is competent to initiate and resolve this

procedure the Director of the Spanish Data Protection Agency.

Likewise, article 63.2 of the LOPDGDD determines that: "The procedures processed

by the Spanish Data Protection Agency will be governed by the provisions of the

Regulation (EU) 2016/679, in this organic law, by the provisions

regulations dictated in its development and, insofar as they do not contradict them, with character

subsidiary, by the general rules on administrative procedures."

II

Regarding the facts that are the subject of the original claim dated 08/19/2020, and its extension

through the writings of 06/04 and 08/2021, referring to deliveries of documents without due

consideration of confidentiality, or reservation, it should be noted that it was already resolved and

pronounced the AEPD on these issues by means of a resolution of inadmissibility to

procedure that was not appealed.

In the extension to the original claim, through the writings of 06/04 and 08/2021, it is

reveal new facts. In some, the evidence provided as the mere

presence of a third party, an employee, before the person delivering the document, without

reveals access to it, or the statement that the document was delivered openly,

by an employee, are not sufficient to understand the illegitimate interference in the

right to data protection, in this case in the development of employment functions

public that the claimant develops. In other cases, there is a delivery of

Work documents. Finally, contact information such as the telephone number, which are considered

in the treatment of personnel management, given the exceptional situation and functions of the

set to develop. These statements alone do not constitute conclusive evidence.

to impute a breach of confidentiality in the course of the usual performance of the

functions.

II

Regarding the claim of 06/08/2021, referring to the use of the fingerprint from the

03/13/2020, 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 dactyloscopic data;”

The scope of application of the GDPR extends its protection, as established in its article 1.2, to the fundamental rights and freedoms of natural persons and, in particular, their right to the protection of personal data, defined in article 4.1 as "all information about an identified or identifiable natural person (“the data subject”); HE An identifiable natural person shall be considered any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a name, an identification number, location data, an online identifier, or one or various elements of physical, physiological, genetic, psychological, economic, cultural or social of said person.”

Each individual has unique fingerprints that show specific characteristics. that can be measured to decide if a fingerprint corresponds to a sample registered. Biometric data present the particularity of being produced by the user himself. body and definitely characterize it. Therefore, they are unique, permanent over time. and the person cannot be freed from them, they can never be changed, not even with age, creating liability issues in case of compromise-loss or intrusion into the system.

These are data whose use may lead to significant risks for the rights rights and freedoms, and therefore one of the so-called "special category", although not defined by the GDPR, in principle their treatment in the article is prohibited 9.1 of the GDPR.

A similar situation of prohibition is contemplated in the Recommendation CM/Complainant (2015) 5, from the Council of Ministers of the Council of Europe to the Member States on the processing of personal data in the employment context. Specifically, principle 18 of this Recommendation establishes the following: “18.1. The collection and further processing of biometric data should only be undertaken when interests are to be protected

legitimate businessmen, employees or third parties, only if there are no other means less intrusive materials available and only if accompanied by the appropriate guarantees provided for in the principle 21. 18.2. The processing of biometric data must be based on methods scientifically recognized and must be subject to the requirements of strict security and proportionality".

A special reference to biometric data is made in opinion 4/2007 on the concept of personal data adopted on 06/20 by GT 29 (this Group was created by virtue of of article 29 of Directive 95/46/EC. It was a body of the EU, of a consultative and independent, for data protection and the right to privacy. Its functions are described in article 30 of Directive 95/46/EC and in article 15 of Directive tive 2002/58/CE), which indicates: "These data can be defined as biological properties, physiological characteristics, personality traits or tics, which are, at the same time, attributed buible to a single person and measurable, even if the models used in practice to measure them technically imply a certain degree of probability. typical examples of Biometric data are those provided by fingerprints, retinal models, facial structure, voices, but also the geometry of the hand, the venous structures and even a certain deeply ingrained ability or other characteristic of behavior behavior (such as handwriting, heartbeat, a particular way of walking or speaking, etc.). A particularity of biometric data is that they can be considered both as content of information about a certain person (So-and-so has these fingerprints) useful) as an element to link information to a certain person (this

object has been touched by someone who has these fingerprints and these fingerprints co-

they respond to so-and-so; therefore so-and-so has touched this object). As such, they can serve

of "identifiers". Indeed, since it corresponds to a single person, the biometric data

can be used to identify that person. This dual character also occurs in the case

of DNA data, which provide information about the human body and allow

have the unequivocal identification of one, and only one, person."

Determines article 9 of the GDPR:

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

race, political opinions, religious or philosophical convictions, or trade union membership,

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

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

sexual orientation of a natural person."

Section 2 establishes the exceptions that must occur so that it can

be carried out, which in labor matters, with various conditions in its articles, would be:

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

following:

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

personal data for one or more of the specified purposes, except when the Law of the

Union or of the Member States establishes that the prohibition mentioned in paragraph

1 cannot be lifted by the interested party;

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

specific rights of the controller or the interested party in the field of

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

Union or Member State law or a collective agreement pursuant to

Law of the Member States establishing adequate guarantees of respect for the

fundamental rights and interests of the interested party;”

[…]”

"4. Member States may maintain or introduce additional conditions, including

limitations, regarding the treatment of genetic data, biometric data or data

relating to health."

So, first of all, to enable the processing of biometric data, you must

comply with any of the specific cases of authorization of this type of treatment

conformed by the regime of article 9.2, letters a) to j), being the closest to the scope

employment that of letter 9.2.b) and in addition to the circumstance that raises the

prohibition of treatment, one of the legitimate bases must concur so that the

data processing is lawful, which are defined in article 6.1 of the GDPR, and comply with the

principles that are expressed in article 5 of the GDPR, among which play an important role

the minimization and proportionality and need to process these data.

Article 6.1 of the GDPR states:

"1. Processing will only be lawful if at least one of the following conditions is met:

a) the interested party gave his consent for the processing of his personal data for one

or various specific purposes;

b) the treatment is necessary for the execution of a contract in which the interested party is

party or for the application at his request of pre-contractual measures;

c) the processing is necessary for compliance with a legal obligation applicable to the

responsible for the treatment;

d) the processing is necessary to protect vital interests of the data subject or of another

Physical person;

e) the treatment is necessary for the fulfillment of a mission carried out in the interest

public or in the exercise of public powers conferred on the data controller;

f) the treatment is necessary for the satisfaction of legitimate interests pursued by the user.

responsible for the treatment or by a third party, provided that such interests are not

the interests or fundamental rights and freedoms of the data subject prevail

require the protection of personal data, in particular when the data subject is a child.

The provisions of letter f) of the first paragraph shall not apply to the treatment carried out

by public authorities in the exercise of their functions."

Article 7 of the Charter of Fundamental Rights of the European Union, proclaimed by

the European Parliament and the Council of the European Union and the Commission of 7/12/2000, pres-

Crites that everyone has the right to respect for their private life, and article 8.1, that all

person has the right to the protection of personal data that concerns him. In-

interpreted jointly, it is inferred that it may constitute a violation of such rights.

chos any data processing, in this case the claimed. This use of data

as employees of the defendant, with the means and ends decided by the same, under

their conditions, supposes an intrusion of their right to private life and to the protection

of data if it is not justified. Article 8.2 of the Charter of Fundamental Rights

specifies that personal data can only be processed with the consent

of the interested party or by virtue of another legitimate basis provided by law. In addition, the articles

7 and 8 of the Charter are not absolute, admitting limitations, as long as they are foreseen

by law, respect the essential content of those rights and with observance of the principle of proportionality, are necessary and respond effectively to objectives of general interest. recognized by the Union or the need to protect the rights and freedoms of others (Judgment of the Court of Justice of the European Union, fourth room, judgment of 10/15/2013, C/291/2012.). These aspects, moreover, are reiterated in relation to the fundamental rights, in art. 52.1 in fine of the Charter of Fundamental Rights of the EU.

The analysis of the legitimacy of biometric processing must be based on a legitimizing, but also if the treatment is necessary, proportional and can be carried out carried out with a low risk to the rights and freedoms of the interested parties.

In this case, it refers to data processing through the fingerprint registration system for compliance with the time control record, east control, which is established as obligation in the field of administration claimed by the Order of 09/07/2009, of the Ministry of Public Administrations and Justice, on working hours and holidays of civil servants. This Order, as an administrative provision, complements "the Agreement between the Administration of the Junta de Comunidades de Castilla-La Mancha and the trade union organizations, which establishes the Plan for the reconciliation of life family and labor of the public employees of the Administration of the Board of Communities of Castilla-La Mancha" which provides in its section 5, the adaptation and Modification of the norms regulating the regime of work schedules of the different sectors of public employment, in order to incorporate rationalization criteria and flexibility of the working day that allow the best possible way to reconcile the daily working day with family life, without diminishing the adequate provision of public services. The Order establishes for the centers and offices of the Administration of the Junta de Comunidades de Castilla-La Mancha and its public bodies: "providing itself with the electronic or computerized means suitable for the control of the personnel schedule". No

indicates or imposes the specific instrument or system to be used, and the need is not discussed

to do this type of control, but to do it through the proposed technique, that is, the

use of identification systems based on biometric data and the determination of the

necessity and proportionality thereof.

Regarding the object of the claim itself, the statement of the claimant that it does not

consent was requested by the defendant for the system of taking and using the fingerprint

fingerprint as a record of working hours, it is indicated that consent is only one of the

causes that would enable the processing of these data, although "it is very unlikely that the

Consent constitutes a legal basis for data processing at work, unless

unless the workers can refuse without adverse consequences [...] (opinion 2//017

on data processing at work, of the Article 29 Working Group).

Regarding the manifestation of the defendant that its time control system was adjusted in

Regarding the legitimizing basis, to the provisions of article 6.2 of the LOPD 15/1999;

"2. Consent will not be required when personal data is collected for

the exercise of the functions of public administrations within the scope of their

skills; when they refer to the parties to a contract or pre-contract of a relationship

business, labor or administrative and are necessary for its maintenance or compliance.

It must start from the basis that said LOPD is a development of Directive 95/46, of the

European Parliament and of the Council of 10/24/1995, regarding the protection of persons

with regard to the processing of personal data and the free circulation of these

data, which established in its article 7 the principles related to the legitimacy of the

data processing, in a similar wording to article 6 of the GDPR, indicating that:

“Member States shall provide that the processing of personal data may only

take place if:

a) the interested party has unequivocally given his consent, or

b) it is necessary for the execution of a contract in which the interested party is a party for the

application of pre-contractual measures adopted at the request of the interested party, or

c) it is necessary for the fulfillment of a legal obligation to which the

responsible for the treatment, or

c) it is necessary to protect the vital interest of the data subject, or

d) it is necessary for the fulfillment of a mission of public interest or inherent to the

exercise of public authority vested in the data controller to a third party to whom

communicate the data, or

e) it is necessary for the satisfaction of the legitimate interest pursued by the person responsible for the

treatment or by the third party or third parties to whom the data is communicated provided that it does not

the interest or fundamental rights and freedoms of the data subject prevail

require protection pursuant to Article 1(1) of this Directive.”

The competences related to time control are not developed in such a way that

determine the instrumental means to carry them out, influencing a right

of their owners, so any interference in them must be

expressly provided for in a Law. In this case, the determination of the exercise of

competences is an unspecific term that does not imply per se but only the end, not the

media. Likewise, the Law containing said mention should establish the guarantees

for the treatment of the rights of people. For the rest, being precise the control

schedule, maintenance or compliance thereof does not depend on the establishment and use of

the fingerprint, a physical bodily element owned by the sole employee, on which

imposes the obligation of use, imposing your collaboration to be collected and used, as

mandatory, without a legal norm that expressly imposes it.

The day registration system for time control through the fingerprint can

have advantages, but it is not the only one that makes it possible to guarantee it. One would have to question whether it is

necessary

processing is necessary in relation to the purpose pursued and objective proportionality

of the treatment, since the limitation of the fundamental right to the protection of personal data

nals must be strictly necessary. This implies that if the achievement of the goals

planned can be carried out without processing personal data, this route will be preferable and sup-

It will state that it is not necessary to carry out any data processing. Appreciated that the recog-

protection, storage and use of data is necessary, this constitutes per se a limitation of the

data protection right.

This therefore requires, first of all, analyzing and ensuring that data collection is

necessary for the established or intended purpose and if so, that it be proportional.

For this purpose and as an example, already on 10/10/2017, the EDPS-European Protection Supervisor

de Datos, an independent supervisory authority whose main objective is to guarantee

that the institutions and bodies of the European Union respect the right to privacy and

data protection when they process personal data- did not consider it proportionate

the use of the biometric fingerprint system for the control of work personnel and exit from the

personnel in the European Parliament, as it is not considered necessary or proportional in relation to

with the purpose, which could be achieved with less intrusive means

(https://edps.europa.eu/sites/edp/files/publication/20-10-

07_edps_biometrics_speech_en.pdf),

https://edps.europa.eu/data-protection/our-work/publications/supervisory-opinions/use-computerized-system-european_en.

and

Regarding the face-to-face control that is carried out with the fingerprint, the people who who telework can clock in on those days using the computer, and in the period of pandemic this system was in force, temporarily replacing the fingerprint. Without However, the use of the footprint has been resumed. However, it does not give a clear explanation of that a person be allowed to use numerical codes without a fingerprint, because he refused to give it, at the same time that it explains that this mode exists in case the trace fails. With it, it reveals that there is an unfounded differentiation of treatment that is not recorded offered to the rest of the employees, and that it is feasible at least another means of control to the footprint, without prejudice to the fact that the defendant did not respond to the option that resulted from the risks which pointed out:

“Opt for 1:1 biometric verification or authentication systems, using the formula of combine code plus footprint in all cases. In addition, it is recommended that systems are based on the reading of the biometric data kept by the worker, for example on a card.

An alternative to use is not a measure designed for when the one foreseen fails, but rather It must be, initially, a double option. An employee uses a code because registration was refused and use of the fingerprint, facilitating the measure that was given to the rest of the employees verbally, a fact that cannot be proven to have been given to the other employees, given that the duty to document decisions in matters of data processing have to be documented, and verbally it is a mere manifestation that does not even have to have occurred, nor that it has been given to all employees, and in any case, it is difficult to proof.

IV.

In accordance with the GDPR article 5, paragraph 1, letter a), in addition to the obligation that the data are treated lawfully and fairly, transparency is included as a fundamental aspect of these principles.

Transparency is intrinsically linked to loyalty and the new principle of responsibility. proactive quality of the GDPR. Furthermore, from Article 5(2), it also follows that Data controllers should always be in a position to demonstrate that data controllers personal data is processed in a transparent manner in relation to the data subject. The princi- responsibility requires the person responsible to take responsibility for what they do with personal data and how it complies with the other principles, and must have measures appropriate days and records to demonstrate compliance.

In accordance with recital 171 of the GDPR, "all treatment already started on the date of application cation of these regulations must conform to these regulations within two years from the date of its entry into force" and those responsible for the treatment must ensure that it complies with its transparency obligations as of the 05/25/2018 (in addition to the rest of the obligations under the GDPR). This implies that, before 05/25/2018, data controllers should review all the information provided to the interested parties on the processing of their personal data in order to ensure they meet transparency requirements. When changes or additions to such information, data controllers should make it clear to data subjects terested that these changes have been made to comply with the GDPR. The GT29 rec-

It is recommended that these changes or additions be actively brought to the attention of the interested parties.

data, but, at a minimum, data controllers must put this information

publicly available (eg on your website). However, if the changes or additions are

important or substantial, these changes should be actively brought to the attention of the

interested.

When data controllers act with transparency, this empowers stakeholders

designed to hold data controllers and processors to account and to exercise

control over your personal data.

The transparency requirements contained in the GDPR apply regardless of the

legal basis for the treatment and throughout the entire life cycle of the same. this remains

patent in article 12, which provides for transparency to be applied in the following stages

of the data processing cycle:

• before the data processing cycle or at the beginning of it, that is, when they are collected

personal data through the data subject or by other means;

• throughout the entire processing period, that is, when they are communicated to the interested parties.

two his rights; and

• at specific times while treatment is in progress, for example, when

data security breaches occur or in the event of changes

important

In addition to the changes in the obligations of transparency, the principles of loyalty and res-

proactive responsibility affect the rights of data subjects with the application

and entry into force of the GDPR. The new categorization of biometric data into statistical data

treatment and its initial prohibition of treatment, supposes not only that the

communication of the new elements of transparency in the treatment carried out

since 2016 to the substantial aspects involved with the modification in the privacy policy

vacancy of the fingerprint treatment, special category that as specific risks that

entails its treatment, it must have safeguards differentiated from other categories.

streams of data With such forecast, it cannot be indicated that there is no legal certainty in the

anticipation than the prohibition with considerable anticipation established by the GDPR. Without

that it is prejudged that the fact that a system was initially implemented did not

may imply that it is updated to what is required as mandatory with a change in the regulations,

to which they have had time to adapt.

V

The GDPR makes the application of all the compliance measures that it provides for

responsible and in charge, of the level and type of risk that each treatment implies for the

rights and freedoms of those affected. Article 28 of the LOPDGDD, states as obligatory

tions:

1. Those responsible and in charge, taking into account the elements listed in the

Articles 24 and 25 of Regulation (EU) 2016/679, will determine the technical measures and

appropriate organizational measures that must be applied in order to guarantee and prove that the treatment

is in accordance with the aforementioned regulation, with this organic law, its rules of

development and applicable sectoral legislation. In particular, they will assess whether the realization

of the impact assessment on data protection and the prior consultation referred to in the

Section 3 of Chapter IV of the aforementioned regulation.

Article 32 of the GDPR also indicates as one of the factors to be taken into account, "the

risks of variable probability and severity for the rights and freedoms of individuals

physical" for the application of appropriate measures to guarantee "a level of security

appropriate to the risk.

The paradigm shift with the previous regulations operated with the RGPD is proof of the fact that

that the requirement that security measures must be adapted to the characteristics

characteristics of the treatments, their risks, and the context and technology in which the treatment is carried out.

state of the art and costs. This would contrast with the LOPD prior to the GDPR, which based

I knew the security measures, basically taking into account the type of data that was processed. The

application of the measures now cannot automatically derive from the fact that some

or other data, but must be the consequence of a specific risk analysis for

each treatment.

Risk management related to data processing operations subject to the

GDPR implies that all decisions related to said treatment, and not only

linked to their safety, must be based on risk management.

There is always an inherent risk to the treatment, due to the very fact of carrying it out, for

Therefore, what the risk management process pursues is to keep them identified, evaluated

and treat them, establishing a response to them, adopting the necessary safeguards.

measures to reduce said risks to a level considered acceptable.

In the context of the AA.PP. , apart from focused risk analysis methodologies

in information security, they have to be expanded to include risks associated with non-compliance

compliance with the provisions of the GDPR, insofar as they are responsible for the treatment of

the data of citizens, or their employees. Before launching new activities

data treatment or modify services already provided that make use of new technologies

guidelines, they must identify those risks to which the treatment may be exposed. By

For this reason, all treatment, both the existing ones and those that are intended to be initiated, must be obtained

subject to a risk analysis. Risks that are not static, continually evolve,

therefore, once identified, it requires a permanent supervision effort. The attitude co-

The right way is to know the risk, assess its consequences, take steps to minimize it, and

monitor its effectiveness in a changing context. This continuous monitoring scheme is

what is defined as risk management.

The risk must be determined on the basis of an objective evaluation, through which it is determined

terminate if data processing operations pose a high risk. A high risk is

a special risk of harm to the rights and freedoms of the interested parties.

The evaluation, management and minimization of the risk to rights and freedoms is a

obligation of the controller (articles 23.2.g, 24.1, 25, 32, 33, 34, 35 and 36

among others of the GDPR) and is part of the regulatory compliance list. the GDPR,

Although it gives some indications, it is not specific when it comes to identifying and establishing how

Perform risk management for each treatment specifically.

The defendant provides a copy of the "security measures that guarantee that the data per-

personnel present the minimum security risks, according to the risk analysis carried out"

attached as ANNEX IV, carried out on 01/16/2021, with the GESTIONA tool

of the AEPD. Regarding this assessment, the following must be specified:

-It is a tool to help with regulatory compliance that aims to support the decision-

sion and whose use generates the basic documentation, in no case exhaustive on the

that an analysis and risk management must be carried out by those responsible for compliance

with the provisions of the GDPR and LOPDGDD. This basic documentation will be a starting point

given that it must be completed following the indications of risk management and evaluation of

impact on personal data processing.

-It is a tool aimed at SMEs, not at Public Administrations, which are subject to

different, with different risk profiles in the treatment with the addition that it can imply

provide treatments to a wide group, with the impossibility in many cases of

oppose, affecting rights and freedoms, such as among others: proportional reduction

salary as service time not worked or not justified through the system

registration of the day with the fingerprint implanted before the entry into force of the

GDPR, with the LOPD, and therefore can produce effects on the rights of employees.

two.

The Guide for an Impact Assessment on the Protection of Personal Data», which was published in

2014 the AEPD, indicated that there are multiple risk analysis methodologies and they can

be adequate for the objective sought, without including specific guidelines in that area.

to. But due to its relevance and adaptation to the specific case of privacy, mention was made

to the publication "Methodology for Privacy Risk Management" of the Commission Nationale de

l'Informatique et des Libertés (CNIL), to MAGERIT (Methodology of Analysis and Management of

Risks of Information Systems), a tool created by the Higher Council of

Electronic Administration to assist the various public bodies in this area, to

Risk IT (ISACA) or ISO 27005, and also highlighting for these purposes the usefulness of the standards

plus ISO 31000 on risk management principles and guidelines and ISO 31010 on

Risk Management Techniques, detailing various methods that can help

to identify and detect the risks of a new product or service.

-What is provided by the claim of the security measures of the treatment referring to the

risks, does not take into account the fact that the risks to be assessed in relation to safety

are only one of the aspects to be covered, ignoring the management of rights risks.

rights and freedoms in the field of personal data processing, as well as the effectiveness and

effectiveness of the legal and technical guarantees applied.

-You have not evaluated less intrusive options such as the one included:

“Opt for 1:1 biometric verification or authentication systems, using the formula of

combine code plus footprint in all cases. In addition, it is recommended that systems

are based on the reading of the biometric data kept by the worker, for

example on a card.

SAW

It can be deduced from the analysis carried out up to now that quality data is being processed.

personal character of special category, thus considered by the GDPR.

The proactive responsibility system implemented by the GDPR, focused on the management

of the potential risks associated with the treatment, imposes on those responsible for the

treatment that analyze what data they treat, for what purposes and what type of treatment

carry out, relating the potential risks to which they are exposed and from there,

decide what measures to take and apply to ensure compliance based on

of the risks detected and assumed.

The impact assessment on the protection of personal data, EIPD, is the tool that

in the GDPR deals with the guarantee of compliance with this aspect of the treatment.

In the text of the GDPR there is no definition for the term "impact assessment related to

protection of data" or EIPD. Working Group 29, GT 29, created in accordance with

compliance with article 29 of Directive 95/46/EC, independent advisory body of the EU

in terms of data protection and privacy with functions described in article 30 of

Directive 95/46/CE and in article 15 of Directive 2002/58/CE. develop the definition

of EIPD in the WP248 Guidelines on the impact assessment related to the protection of

data and to determine whether the treatment is likely to carry a high risk for the purposes of the

GDPR, adopted on 4/04/2017 and last revised and adopted on 10/4/2017, as:

"…a process designed to describe treatment, assess its need, and provide-

quality and help manage risks to the rights and freedoms of natural persons

derived from the processing of personal data, evaluating them and determining the measures

to address them." According to this, the EIPD is a "process" and, therefore:

• Reducing the EIPD to a specific and isolated activity in time is incompatible with the con-

process concept that interprets the WP248 Guidelines.

• The EIPD must be documented, but the EIPD is more than the report that reflects its re-

results.

• The EIPD must assess the risks "determining the measures to address them". The EIPD

obliges the person responsible to act and has a greater dimension than a mere plastic formalism.

in a document on which minimal changes can be made to adapt it to

any treatment.

The EIPD is a process of analysis of a treatment that extends over time, throughout

of the entire life cycle of personal data processing, and that must be reviewed

continues, "at least when there is a change in the risk represented by the operations

purposes of treatment" (art. 35.11 of the GDPR).

The GDPR imposes the obligation to have a Protection Impact Assessment

of Personal Data (EIPD), determining its article 35 of the GDPR:

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

gies, by their nature, scope, context or purposes, entail a high risk for the rights and

freedoms of natural persons, the person responsible for the treatment will carry out, before the treatment
treatment, an assessment of the impact of processing operations on the protection of
personal information. A single assessment may cover a number of processing operations.
similar behaviors involving similarly high risks.

2. The person responsible for the treatment will seek the advice of the protection delegate
data controller, if appointed, when conducting the protection impact assessment
of data.

3. The impact assessment related to data protection referred to in paragraph
c 1 will be required in particular in case of:

a) systematic and exhaustive evaluation of personal aspects of natural persons who are
based on automated processing, such as profiling, and on the basis of which
make decisions that produce legal effects for natural persons or that affect them
have significantly similarly;

b) large-scale processing of the special categories of data referred to in the article
Article 9, paragraph 1, or personal data relating to criminal convictions and offenses to
referred to in article 10, or

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

4. The control authority will establish and publish a list of the types of operations of
treatment that require an impact assessment related to the protection of personal data
accordance with paragraph 1. The supervisory authority shall communicate these lists to the Committee at
referred to in article 68.

5. The supervisory authority may also establish and publish the list of types of tra-
treatment that do not require data protection impact assessments. The
control authority will communicate these lists to the Committee.

6. Before adopting the lists referred to in paragraphs 4 and 5, the supervisory authority
The competent authority will apply the coherence mechanism contemplated in article 63 if those lists

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

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

members, or processing activities that may substantially affect the free circulation

relation of personal data in the Union.

7. The evaluation must include at least:

a) a systematic description of the intended processing operations and the purposes

of the treatment, including, where appropriate, the legitimate interest pursued by the person in charge

of the treatment;

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

with respect to its purpose;

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

referred to in paragraph 1, and

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

and mechanisms that guarantee the protection of personal data, and to demonstrate the con-

accordance with this Regulation, taking into account the rights and legitimate interests

of interested parties and other affected persons.

8. Compliance with the approved codes of conduct referred to in article 40

by the corresponding managers or managers, due consideration will be given to the

assess the repercussions of the processing operations carried out by said controllers

officers or managers, in particular for the purposes of the impact assessment relating to the protection

tion of data.

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

sentantes in relation to the planned treatment, without prejudice to the protection of interests

public or commercial or the security of processing operations.

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

have their legal basis in Union law or in the law of the Member State that is

applies to the data controller, such Law regulates the specific processing operation

operation or set of operations in question, and an evaluation of the impor-

pact on data protection as part of a general impact assessment on

In the context of the adoption of such a legal basis, paragraphs 1 to 7 shall not apply

unless the Member States deem it necessary to carry out such an assessment prior to

treatment activities.

11. If necessary, the controller will examine whether the treatment is in accordance with the evaluation

impact assessment regarding data protection, at least when there is a change in the

risk posed by processing operations."

In development of paragraph 4, the Director of the AEPD, published an indicative LIST not

exhaustive list of types of treatment that require an impact assessment relating to the

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

necessary to perform a DPIA in the majority of cases in which said treatment meets

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

find in the list of treatments that do not require EIPD referred to in article 35.5

of the GDPR."

The list is based on the criteria established by the "GUIDELINES ON THE

IMPACT ASSESSMENT RELATING TO DATA PROTECTION (EIPD) AND FOR

DETERMINE WHETHER TREATMENT IS "PROBABLY HIGH RISK"

FOR THE PURPOSES OF THE GDPR", adopted on 04/4/2017 and last revised and adopted on 10/4/2017, WP 248 rev.01 of GT 29 that complements them and should be understood as a non-exhaustive list:

The list states:

"4. Processing that involves the use of special categories of data to which it refers article 9.1 of the GDPR, data related to criminal convictions or offenses to which refers to article 10 of the GDPR or data that allows determining the financial situation or patrimonial solvency or deduce information about people related to categories data specials.

5. Processing that involves the use of biometric data for the purpose of identifying unique way to a physical person."

9. Data processing of vulnerable subjects…"

In the Guidelines, it is stated:

"In order to offer a more concrete set of processing operations that require DPIA due to its inherent high risk, taking into account the particular elements res of article 35, paragraph 1, and of article 35, paragraph 3, letters a) to c), the list that must be be adopted at national level under Article 35(4) and recitals 71, 75 and 91, and other references in the GDPR to processing operations that "are likely to involve are at high risk", the following nine criteria should be considered:

"7. Data related to vulnerable interested parties (recital 75): Treatment of this type of data represents a yardstick due to the increasing imbalance of power between stakeholders. and the person responsible for the treatment, which implies that people may be unable to You cease to authorize or deny the processing of your data, or to exercise your rights. Between the

Vulnerable stakeholders may include children (considered not capable of refusing consciously and responsibly grant or authorize the processing of your data), employees".

The defendant resorts to the establishment of the time control system based on biometric data that are part of the physical identity, that does not change over time, and that requires on the part of its owner, the employee, an active collaboration to register their data and access each time you go to the workplace by placing your finger on the terminal reading, allowing parts of its organs to undergo the necessary operations for the operation of the system. Likewise, you may suffer repercussions on your rights when automated decisions are conditioned as a result of the use of the control system that can affect the employee, for the control of deductions from assets.

The GDPR does not require a DPIA to be carried out for each processing operation that may it entails risks to the rights and freedoms of natural persons. The realization of a DPIA is only mandatory when the treatment is "likely to involve a high risk to the rights and freedoms of natural persons". It is possible that the activities ordinary time control procedures probably do not entail a high risk to the rights and freedoms of the interested parties, but if new technologies are introduced and the person in charge of the treatment has not previously carried out a protection impact assessment of data, or if it is necessary given the time elapsed since the initial treatment, it must be

establish this obligation (recital 89 of the GDPR).

In such cases, the controller must carry out, prior to processing, an evaluation of the impact on data protection in order to assess the particular seriousness and probability

high risk, taking into account the nature, scope, context and purposes of the processing.
ment and the origins of the risk. Such an impact assessment should include, in particular, the
measures, guarantees and mechanisms established to mitigate the risk, guarantee the protection
of personal data and demonstrate compliance with this Regulation". (consider-
rando 90).
"The impact assessment related to data protection must also be carried out in the
cases in which personal data is processed to make decisions regarding natural persons
concrete physics as a result of a systematic and exhaustive evaluation of personal aspects
belonging to natural persons, based on the profiling of said data or as a result of
of the processing of special categories of personal data, biometric data or social data
regarding convictions and criminal offenses or related security measures." (recital 91).
The GDPR establishes the obligation to manage the risk that for the rights and freedoms
of people involves these treatments. This risk arises both from the very existence
of the treatment, as well as by the technical and organizational dimensions of the same. The risk
arises from the purposes of the processing and its nature, and also from its scope and the context in which
which is developed, and requires that those responsible for the treatment apply measures
adequate to guarantee and be able to demonstrate compliance with said regulation, taking into account
taken into account, among other things, "the risks of varying probability and severity for the rights
and freedoms of natural persons' (Article 24, paragraph 1). These rights and freedoms
of the interested parties mainly concern the rights of data protection and privacy.
but they can also imply other fundamental rights, such as the
prohibition of discrimination, freedom of movement, etc. .The obligation of those responsible
responsible for the processing of carrying out a DPIA in certain circumstances must understand
be considered in the context of its general obligation to adequately manage the risks deriving from
vads of the processing of personal data.
The complexity of the risk management process must be adjusted, not to the size of the entity,

the availability of resources, the specialty or sector of the same, but to the possible impact of the treatment activity on the interested parties and the difficulty of the treatment itself.

Biometric processing presents, among others, the following risks, some of which are contemplated in OPINION 3/2012 ON THE EVOLUTION OF TECHNOLOGIES BIOMETRIC of GT 29 of 04/27/2012:

-The definition of the size (amount of information) of the biometric template is a question crucial. On the one hand, the size of the template must be large enough to manage the security (avoiding overlaps between the different biometric data, or substitutions of identity), and on the other, it should not be too large in order to avoid the risks of reconstruction of biometric data.

- Risks involved in the use of biometric data for identification purposes in large centralized databases, given the potential consequences harmful to the people affected.

- It goes without saying that any loss of the qualities of integrity, confidentiality and availability with respect to the databases would clearly be detrimental to any future application based on the information contained in said databases, and would cause also irreparable damage to the interested parties. For example, if the fingerprints of a authorized person are associated with the identity of an unauthorized person, the latter could access the services available to the owner of the fingerprints, without having to right to it. The result would be identity theft, which (regardless of your detection) would make the person's fingerprints unreliable for future applications and,

consequently, it would limit his freedom. The reality of technology is that every day new forms of social engineering generate new vulnerabilities that appear within the framework of the treatment where biometric operations are located, so it is necessary to consider data breach scenarios and determine the impact that a data breach hi e could cause the rights and freedoms of the interested parties. Also, it is necessary know the reality of which breaches are already taking place and which could determine the inadequacy of the biometric technique or of biometrics in general. This implies a continuous evaluation of the treatment based on the facts that are producing.

- The transfer of information contained in the database.

-The illusion can be created that fingerprint identification is always correct,

For this reason, an analysis of the errors that may occur in its use must be included, performance evaluation measures, false acceptance rate- probability that a biometric system incorrectly identifies an individual or fails to reject an individual that does not belong to the group, and rate of false rejection or false negative: the correspondence between a person and his own staff. All this with the effects of power be constituted as full proof with regard to the accreditation of the presence of a specific person in the place where he is, with the relationship of the decisions that legally affect a person, a decision that should be made safeguarding the rights and freedoms and the legitimate interests of the data subject, at least the right to obtain human intervention on the part of the controller, to express their point of view and to challenge the decision.

-Security measures must be adopted for the processing of biometric data (storage, transmission, feature extraction and comparison, etc.) and about especially if the person responsible for the treatment transmits this data through the Internet. The Security measures could include, for example, the encryption of templates and the

protection of encryption keys apart from access control and a protection that

makes it virtually impossible to reconstruct the original data from the

templates.

-Likewise, the WORKING DOCUMENT ON BIOMETRY, adopted on 08/01/2003,

of GT29, believes that biometric systems related to physical characteristics that do not allow

trace (for example the shape of the hand, but not fingerprints) or systems

biometrics relating to physical characteristics that leave a trace but do not depend on the

storage of data held by a person other than the interested party (in other

words, the data is not stored in the access control device or in a database

central data center) create fewer risks for the protection of rights and freedoms

fundamentals of people (You can distinguish the biometric data that is

centralized way of biometric reference data that is stored in a

mobile device and the compliance process is performed on the card and not on the sensor or

when it is part of the mobile device).

-It is generally accepted that the risk of reusing biometric data obtained through

from physical traces left by people inadvertently (for example: footprints

digital) for incompatible purposes is relatively low if the data is not stored

in centralized databases, but in the possession of the person and are inaccessible to

third parties. Centralized storage of biometric data also increases the

risk of using biometric data as a key to interconnect different databases,

which could allow obtaining detailed profiles of a person's habits both at

public as private. In addition, the question of the compatibility of the ends leads us to the

interoperability of different systems that use biometrics. The normalization that

requires interoperability can lead to greater interconnection between databases

data.

- Obvious risks if the technology used does not sufficiently guarantee that the

The template obtained from the biometric data will not match the one used in other

similar systems.

All this, without losing sight of the fact that it is a very intrusive identification system for

the fundamental rights and freedoms of natural persons, among other circumstances

by functioning through artificial intelligence systems that implement algorithms

us to design and read the biometric template, put in relation to the deficiency in the

manufacturing standards for approved systems and certificates of use software, added

to the extension and interoperability of use of these systems.

All these elements contribute to considering the high risk for the rights as probable.

rights and freedoms of natural persons that are mentioned in article 35.1 of the GDPR,

In addition, in this case, two conditions of the list of the AEPD of the article are referred to

35.4 of the GDPR.

Regarding the guarantees to be implemented that must be contained in the EIPD, the Guide "The

data protection in labor relations" of the AEPD contemplates, by way of reference

Ten aspects that can be taken into account.

Regarding the statement of the defendant that the EIPD was not carried out because the system

fingerprint processing processing personal data for the purpose of registering working hours

boral is established on *** DATE.2, under the validity of the LOPD and has not undergone any changes

technological or functional that justifies the realization of this DPIA, it should be added that the Di-

guidelines of GT 29 on the impact assessment related to data protection and for

determine whether the treatment is “probably of high risk” for the purposes of the Regulations.

to (UE) 2016/679 adopted on 4/04/2017, last revised and adopted on

4/10/2017, indicate about the existing treatment operations that "The requirement of

performing a DPIA applies to existing processing operations that are likely to be-

entail a high risk for the rights and freedoms of natural persons and for those who

has produced a change in risks, taking into account the nature, scope, con-

text and the purposes of the treatment”

In addition to the precedent legal basis that shows that it has been executed

an insufficient and inadequate basic assessment of risks to the rights and freedoms

from those affected, it should be added that, in addition, within the context, it is necessary to take into account

note that when it was put into operation, September 2016, it had already published several

months before in the DOUE on 05/4/2016, the GDPR, which had its entry into force arranged on

05/24/2016, applicable from 05/25/2018, therefore the prohibition of the use of bio-data

metric as a general rule was known since before not only its start-up, but

of the publication in December 2016 of the PERSONAL file in which the use was found

of the footprint

Regarding the consideration of biometric data as special data, it must be taken into account

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

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

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

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

Some national authorities suggested, due to their specific nature, adding them to the list of

sensitive data. This certifies that there has been a change of context with the approval of said regulation that especially affects biometric data that passed from data generic data to the category of special data as a novel aspect in said regulations of European application, varying not only the technological means from the eventual implementation of the system for the claimant, but the risks, and their extension in areas of clear affectation to the exercise of fundamental rights, with the consideration that as such protection deserves.

Likewise, the implementation of the system by the defendant in its day does not have to mean Without further ado, it has been legitimized while it has been used, without having had a chance the supervisory authority to rule on whether it complies with the elements that it has to complete this type of treatment.

A DPIA should be perceived as an instrument to help in making decisions regarding treatment, so it is advisable to perform it in the conception and design phases of the treatment. This would comply with the principles of data protection from the start. and helps ensure that selected collaterals are guided by risk management and are implemented during the conception and design phase of the treatment, being integrated into the same and extending to all stages of its life cycle. data protection from the design it is not an additional layer or an element that can be added later.

Therefore, an EIPD may imply that changes must be made in the treatment to introduce modifications, guarantees or measures to reduce risks, it must be carried out beforehand. and during the design phase, and the risk approach involved in the DPIA is a process, not a state.

The defendant did not contemplate the diverse and varied elements that have been indicated in this section in its risk assessment, and has stated that there is no risk or that it is acceptable, and these elements must form part of the aforementioned impact assessment.

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

a budget to which must be added the rest of the legal requirements for the treatment,

legitimizing basis and respect for the fundamental principles of data processing provided for

to in article 5 of the GDPR. The defendant does not certify having complied with this obligation,

estimating that he may have incurred in the aforementioned infringement of article 35 of the GDPR.

VII

The alleged infringement is typified in article 83.4.a) of the GDPR, which indicates:

Violations of the following provisions will be penalized, in accordance with paragraph

do 2, with administrative fines of a maximum of 10,000,000 EUR or, in the case of a

company, of an amount equivalent to a maximum of 2% of the total turnover

annual global of the previous financial year, opting for the one with the highest amount:

a) The obligations of the controller and the person in charge under articles 8, 11, 25 to 39,

42 and 43;”

The LOPDGDD establishes for the purposes of prescription of the infringement, in its article 73.t):

"Based on what is established in article 83.4 of Regulation (EU) 2016/679, it is considered

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

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

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

processing operations in the protection of personal data in cases where

that it is enforceable."

VIII

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

two of the following corrective powers indicated below:

"d) order the controller or processor that the processing operations

comply with the provisions of this Regulation, where appropriate, of a particular

in a manner and within a specified period;”

f) impose a temporary or permanent limitation of the treatment, including its prohibition;

[…]”

Yo)

impose an administrative fine in accordance with article 83, in addition to or instead of the measures

measures mentioned in this section, according to the circumstances of each particular case.

lar;”

"The imposition of this measure is compatible with the sanction consisting of a fine

administration, according to the provisions of art. 83.2 of the GDPR.”

The defendant continues to use the fingerprint without having carried out an evaluation of

impact on that processing operation which is likely to carry a high risk in

the rights and freedoms of employees. Thus, among other issues, they continue without

identify the risks associated with the treatment of the use of the fingerprint for control

schedule, and therefore without being able to mitigate them, there being other modalities that for said purpose

the claim has been established. It is therefore considered, in order to guarantee the rights and

freedoms of the owners of the data, which concurs with the need and justification to adopt

corrective powers that are determined in the operative part.

Article 90.3 of the LPCAP indicates that "the resolution that puts an end to the procedure will be

executive when there is no room for any ordinary administrative appeal against it, and may

adopt in it the precise precautionary provisions to guarantee its effectiveness in

so much not executive"

Considering that the defendant is a public entity that is part of the CCAA of

Castilla La Mancha, article 83.7 of the GDPR states:

"Without prejudice to the corrective powers of the control authorities under article

58(2), each Member State may lay down rules on whether and to what extent

measure, impose administrative fines on authorities and public bodies established

in that Member State.

The "Regime applicable to certain categories of managers or managers of the

treatment" of the LOPDGDD provides in its article 77:

[…]”

2. When the managers or managers listed in section 1 commit any

of the offenses referred to in articles 72 to 74 of this organic law, the

competent data protection authority will issue a resolution sanctioning

the same with warning. The resolution will also establish the measures that

appropriate to adopt so that the conduct ceases or the effects of the infraction are corrected.

would have committed

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

depends hierarchically, where appropriate, and to those affected who had the status of

interested, if any.

(…)

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

autonomous communities the actions carried out and the resolutions issued under

of this article.”

In its section 1 it states

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

are responsible or in charge:

[…]"

c) The General State Administration, the Administrations of the communities

autonomous entities and the entities that make up the Local Administration. "

Therefore, in accordance with the applicable legislation and assessed graduation criteria

of the sanctions whose existence has been accredited,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: SANCTION the DEPARTMENT OF HEALTH OF THE BOARD OF

COMMUNITIES OF CASTILLA-LA MANCHA, with NIF S1911001D, with warning for

a violation of article 35 of the GDPR, in accordance with article 83.4 a) of the GDPR, and

for the purposes of prescription of the offense in article 73.t) of the LOPDGDD.

SECOND: Require in application of articles 90.3 of the LPCAP, and 58. 2.f), of the GDPR,

to the DEPARTMENT OF HEALTH OF THE COMMUNITY BOARD OF CASTILLA-LA

MANCHA, so that within ten days, "temporarily or permanently limit the

treatment" of the time control system by means of the fingerprint, as long as it does not have

of a valid data protection impact assessment of the processing, which takes into account

account the risks to the rights and freedoms of employees and the measures and

adequate guarantees for its treatment, or even if it were carried out, it would be necessary to carry out the

consultation forecast established in article 36 of the GDPR.

After the time granted, you must inform this AEPD.

Failure to comply with the requirement may lead to the commission of a violation of the

article 83.6 of the GDPR,

THIRD: NOTIFY this resolution to the MINISTRY OF HEALTH OF THE

COMMUNITY BOARD OF CASTILLA-LA MANCHA.

FOURTH: COMMUNICATE this resolution to the Ombudsman, in accordance with

what is established in article 77.5 of the LOPDGDD.

FIFTH: In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process 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 replacement 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 Court, with

in accordance with the provisions of article 25 and section 5 of the fourth additional provision

of Law 29/1998, of 13/07, regulating the Contentious-administrative Jurisdiction, in the

period of two months from the day following the notification of this act, according to what

provided for in article 46.1 of the aforementioned Law.

Finally, it is noted that in accordance with the provisions of art. 90.3 a) of the LPACAP, it may be

provisionally suspend the final resolution in administrative proceedings if the interested party expresses

their intention to file a contentious-administrative appeal. If this is the case, the

The interested party must formally communicate this fact by writing to the Agency

Spanish Protection of Data, presenting it through the Electronic Registry of the

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

remaining records provided for in art. 16.4 of the aforementioned LPACAP. You will also need to transfer

to the Agency the documentation that proves the effective filing of the appeal

contentious-administrative. If the Agency were not aware of the filing of the

contentious-administrative appeal within a period of two months from the day following the

Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

938-181022

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es