 File No.: PS/00050/2021

RESOLUTION OF TERMINATION OF THE PROCEDURE FOR PAYMENT

VOLUNTARY

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

to the following

BACKGROUND

FIRST: On February 19, 2021, the Director of the Spanish Agency for

Data Protection agreed to initiate disciplinary proceedings against SERVICES

LOGISTICS MARTORELL SIGLO XXI, S.L. (hereinafter the claimed party).

Notification of the initiation agreement and after analyzing the arguments presented, dated 6

October 2021, the proposed resolution was issued, which is presented below:

transcribe:

<<

File number: PS/00050/2021

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

following:

BACKGROUND

FIRST: The claim filed by the UNION SECTION ***SECTION.1 (in

hereinafter, the claimant) has entry dated 02/06/2020 in the Spanish Agency of

Data Protection from the Catalan Data Protection Authority. The

claim is directed against the company, in which, they state they hold representation

trade union: SERVICIOS LOGÍSTICOS MARTORELL SIGLO XXI, S.L., with CIF B65050247 (in

hereinafter, the claimed one), “because of its opposition to the implementation of a pre-employment

workers through a fingerprint biometric system in the dependencies

information of the company, by means of terminals that incorporate readers for capturing the

fingerprint of each employee", and "currently the system is combined with the reader of

card".

The defendant dedicates its activity to the "assembly transport and assembly of parts of

motor vehicles, being the SEAT company for which they provide services as the only

client" with about 520 workers.

The claimant states that, in his opinion, the system that is in the "testing" phase is not

in accordance with the regulations, by:

Disproportionate: "The company's facilities are located

to)

within the SEAT MARTORELL premises, which has its own action control system.

access, visits and labor presence, to which the workers must submit" of the

called "to which must be added the card transfer system itself established in

the company, so a third control system is disproportionate."

Unnecessary, due to the existence of other less invasive means to reach the

to)

presence control.

It is also intended with the implementation of the system, the control of the pro-

b)

duction by having installed the readers in the work areas.

c)

Absence of consent: the company forces the workers to sign a document

document of consent for the processing of your data, so it is not a manifestation

free will celebration.

SECOND: On 03/26/2020, the claim is transferred to the claimed one, that the

07/09/2020, states:

1) As the company is located within the client's facilities, SEAT, the employees

to access, they have to go through the access control to the factory that its owner has im-

planted. From this point, to the location of the claimed company, there is a path

walking about twenty minutes. Indicates that the work center has a total area

greater than sixty thousand square meters, providing a graph with the location of the points

time registration.

In the spaces where the footprint records are implanted, there were historically two

card presence control terminals, which allowed presence control, and

the control of the working day-entries, exits and absences- and, on the other hand, the generation of

report of variables for the preparation of payroll -overtime, night shifts.

It states that "during 2017, with the idea of replacing these card terminals,

five footprint terminals in each of the center's work areas. These new

terminals came to replace the two card ones with the same purposes and the same information.

mation". This measure is executed with several premises:

-to avoid the problem of staff leaving their jobs before

of the hour and sign at the entrance of the workshop the exit of your shift, and,

- facilitate the signing process by avoiding crowds at signing points, pass-

do from two to five.

He adds that the fingerprint exceeds the card because it avoids cases that have given the card

between employees to sign for the owner.

A single type of record of presence of working hours will be implemented, although currently

the card and the new fingerprint coexist, they are using both to verify that they work.

tion correctly before implanting it definitively. It indicates that they are going to establish a pro-

program to reduce the time in which both systems, card-fingerprint, will coexist, and will

carry out the new explanations of the system to the workers and their representatives.

2) On 11/13/2017, the Company Committee was convened and the project and objectives were presented

presence control by fingerprint, delivering a copy of the report from the provider of the

technology, granting a deadline for it to issue its report. Provide documentation of the record

of the meeting. It indicates that on 11/20/2017, they held a second meeting in which the Sec-

Union of ***SECTION.1, but not the one of ***SECTION.2, was opposed to consider it dis-

provided and stated that the current card system was sufficient and requested a pro-

mediation procedure, which did not come to fruition, and later, on 10/15/2018,

The claimant forwarded the complaint to the Labor Inspectorate. On 01/14/2019, the

complaint for not proving infringement. Provide a copy of these documents.

3) States that the collection of fingerprints and implementation of the system was reported to each

worker, documenting its delivery with receipt. They provide a copy of the of an employee,

which is dated 01/22/2018, with the literal “information from the management of the company

prey and acceptance by the users of the fingerprint record”, “from the direction of the

The human resources department informs the workers that the

implementation of an access control system for visits and labor presence through

fingerprint for which users will be requested to register it and all of this in accordance with

accordance with the provisions of the Personal Data Protection Law 15/99 of

13/12".

4) States that the publication of Royal Decree Law 8/2019 of 8/03, on urgent measures

of social protection and the fight against job insecurity in the working day, intensi-

The tasks of starting up the signing system were established, establishing a period of storage

given four years of recorded data.

5) Provides a graphic diagram of the operation of the fingerprint treatment process

fingerprint indicating:

“After the discharge of the worker and at the time that he is informed of the collection of the egg,

to.

tag to control the day, an HR technician takes the fingerprint with the reader called

***READER.1 (“Minuts-based system: identifies a limited number of

footprint shapes and their position within the footprint. The reader captures the fingerprint and

talizes a few landmarks and converts the minutiae into a footprint template.

frada (algorithm)”.

“Fingerprint images are never stored. This footprint template does not allow

biometric identification, only biometric verification”

b. After taking the fingerprint, it appears that the "human resources technician associates in

program ***PROGRAM.1 the fingerprint template with employee ID”. In the drawing

of ***PROGRAM.1 states that “stores data on the server; employee ID, name

name and surname, NIF, encrypted fingerprint template, date, check-in time, check-out time, absence

whoa“.

c. From ***PROGRAM.1 there is a double date to TIMETABLE, and from this to

***PROGRAM.1. On the RECORDER, it appears: “the worker records”. From

***PROGRAM.1 to RECORDER contains: “TCP automatic transfer of frame

extra decimal: employee ID, name and surname, encrypted fingerprint template”. From FI-

CHADORA, in which it appears: "Stores data on the device: employee ID, template-

the encrypted fingerprint", the arrow appears to ***PROGRAM.1, appearing: "Automatic transfer

matic TCP extradecimal frame: employee ID, date, entry time, exit time, auth.

sentences".

There is an explanatory parenthesis below TIMETABLE, indicating:

"User verification is performed locally against the encrypted template stored on the file.

chadora. It is never verified against the central database of ***PROGRAM.1. They are collected

automatically the date and time data. The worker registers manually with a code

the absences".

In the explanatory graph, another screen also shows the flow when the drop occurs

of the employee.

6) States that analyzing the reports of the Legal Office of the AEPD number

65/2015, 36/2020, of 05/08, and opinion 3/2012, of the Article 29 Group, on "evolution

of biometric technologies" the difference of biometric data is concluded:

-"The biometric identification: The identification of an individual by a biometric system

is normally the process of comparing your biometric data (acquired at the time

of identification) with a series of biometric templates stored in a database.

tos (i.e. a one-to-many correspondence search process."

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

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

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

(i.e. a one-to-one mapping process)."

"They would only be treated as special category data, those in which they are submitted to

technical treatment aimed at biometric identification "one to many", and not in the case of

one-to-one biometric verification/authentication.

They state that their system is verification/authentication, explaining that only the

correspondence of the biometric data provided at the time of registration for the interest

sado to prove that it is him. “This data is stored on the device in encrypted form

and is queried by the authentication system to verify that there is a match.

“When an employee puts his finger on the reader of the time card, this device verifies

locally, never against the central database, which corresponds to the fingerprint template

encrypted that is stored on the device. In case there is a match,

collects the clocking data - date, time, employee ID, absence, etc. - and sends them to the program

transfer management program ***PROGRAM.1. This is an authentication, similar to the one

zed with a password”.

7) States that to date no employee has exercised any type of right with respect to

your data.

8) Provide a copy of the risk analysis of treatment activities, (questionnaire model and

notes to it). “Applying as a first step the adaptation of the FACILITA tool

RGPD on 04/08/2019 the result of the "low risk" activity is obtained. Indicates that

evaluated the need to carry out or not an DPIA. “The result determined that it was not specified

knew how to carry out a data protection impact assessment (DPIA) precisely because of the

interpretation that the fingerprint template encrypted by the algorithm should not frame

be included in specially protected data”.

But if a “basic risk analysis” was carried out “to determine if it was necessary to implement

additional processes and protocols to those designed”:

-“09/16/2019, review of the probability of risk number 5 due to improvement opportunity

in the deletion process detected as a result of the implementation plan of ISO 27001 passes evaluation

tion”.

-In the section specifying the categories of data processed: "Data of

personal identification character, fingerprint template, and employee: name and

surnames and NIF. In addition, date of entry and exit, and absences are treated.

The conclusion of the analysis indicates: "it is of little risk", "when an employee puts his finger

in the card reader, the device itself verifies that it corresponds to the template of

the fingerprint that is stored in the device. In the event that there is coincidence

cia, collects the clocking data: date, time, employee ID, absence, etc., and sends them

to the transfer management program ***PROGRAMA.1”.

”It is considered that it is an authentication similar to that carried out with a password.

password and not a biometric identification, so it is not considered a data especially

protected how will be the complete image of a fingerprint that will allow to identify a worker

dor inside a whole bag of people.”

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

process the claim filed by the claimant on 09/7/2020.

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

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

11/23/2020, your collaboration was requested, to report on the registration system of

imprint they use.

1) They are asked to briefly explain how the registration and storage system is produced.

da-template storage What is ***PROGRAM.1?, what is the central base of

***PROGRAM.1?, and if the template converted into an algorithm for each employee is saved there,

and what relationship does it have with the device called "tagging machine"

On 12/15/2020, your response is received in which you state:

***PROGRAM.1, “main server for the management of the presence system, belongs to the

"Grupo Sesé", the same group to which the claimed belongs and is implemented through a

commercial application called ***PROGRAMA.1, from the company TECISA”.

for management is stored in a database included with the application, and it is in this

database what the application has, where the template collected from the

fingerprint".

The recorder, or remote terminal “acts as an interface between the employee and the ***PRO-

GRAMA.1 for the validation and collection of information”. Through this device, “we validate

we give in the system and collects information such as the time in which we have interacted, for

example".

2) In the graphic drawing of the process “The worker records”, and “recorder”, the literal “al-

stores data on the device: employee ID-encrypted fingerprint template”, in this sense, clarify

what device are you referring to? to the recorder?, describing if that were how it is stored

the staff of all employees in each and every one of the five that they have.

He distinguishes two phases of the process, the data registration phase and the operation phase of

presence record.

Phase 1, Data Recording:

-Human Resources registers the employee's data and collects his fingerprint with a reader (denoted-

mined in this case ***READER.1). “At the time of capture, a template is generated

with the characteristic points of that footprint, which is stored encoded in the database

***PROGRAM.1. The fingerprint image is not stored.

When the data is written, the synchronization process sends the necessary data from

the application ***PROGRAMA.1 to the associated registers -five- where they are stored-

two such values. The data that is sent is the ID of the employee, name and surname and the

encrypted template."

Phase 2, Operation:

-"When an employee wants to register his presence, he places his finger on the recorder that me-

through the built-in ***READER.1 reader, it performs the same process mentioned in phase 1

when the employee was registered in the system. So you take a screenshot of the

characteristic points of the employee's footprint, this capture is encoded and compared with

the encoded template which is stored in the memory of the recorder and associated with the ID

of the employee. If it is correct - both templates coincide - the recorder will send the pertinent data.

employee's necessities. The coded fingerprint or the name is never sent, only information is sent.

information relevant to the clock: date, time, employee ID and any defined code of

absence. This data is what is transmitted to the ***PROGRAM.1 application to

its subsequent processing.

3) About your manifestation of:

"User verification is performed locally against the encrypted template stored on the file.

chadora. It is never verified against the central database of ***PROGRAM.1"

You are requested to provide more information on:

to)

If your system uses the same template for each employee, recording different al-

goritmos, or different templates for each employee.

He states that when mentioning template "it is actually the encrypted information that

has been saved after reading the fingerprint, the fingerprint is not stored as an image, but is detected

and they keep between 25 and 80 minutiae - they are the points of the trace where a line ends or

branches- these points are the ones that are encoded and stored as a template. Each one of

we have some points differentiated from each other, which is enough to be able to

identify us and what is saved are these points, so there cannot be two codes

identical.”

to)

Explain how it is possible to correlate through the system one-to-one (authentication)

tion) the introduction of the fingerprint in the recorder, with the template(s), explain if all the

template/s are found in the recorder. (apparently fingerprint validation will occur)

translated versus all templates.)

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

It reiterates that “Each recorder stores the templates and the ID of each employee, so

when an employee puts the fingerprint it is encoded in a template and the system performs the

search to see which one is equal to the one generated. The process is carried out locally, it is not

consult the application ***PROGRAMA.1”

b)

What difference would there be between the worker registering in the recorder and the verification being

does it locally against the encrypted template stored in the recorder, as long as it does it against

the central database of ***PROGRAM.1?

“There would be no technical difference or practicality. The process would be the same, only in that

In this case, it should be compared with all the stored templates and it would increase significantly.

Mind the time it would take to transmit the information back and forth.

c)

Does the recorder have at any time a single packet of data identifying the

person who is clocking or all the packages of all the workers?

He answered that “The register keeps the information of all the workers of the center, since

that have been configured to facilitate the signing in any of them by the worker.

pain”.

4) In the graph, from "tab" to "***PROGRAM.1", there is a double arrow in which

literals are contained: “automatic transfer, extradecimal frame TCP etc.”, it is requested

that explain the meaning of these extremes in both directions, and that imply the two

possible arrows, if it could be understood that there is a transfer of data from the system

ma central to the recorder. (employee id-name/surname-fingerprint).

It reiterates that: “When an employee is registered or modified, it is done from the

application ***PROGRAM.1. Once the data is saved, the system launches an update.

tion to the recorders through a TCP frame where the information is transmitted (name

employee name, employee ID, fingerprint template) remaining registered in the fi-

chadoras”.

Only when an employee makes a clocking in the register and after the validation process

tion, the recorder, sends the information (ID, date and time, absences) to the application of

***PROGRAM.1”.

They indicate that your system works like that of a password. To this end, they must detail the

elements of said idea, user, how it is verified and what would be the password element,

how, and where they are stored and how and against which element the matching occurs.

He answers that comparing the traditional way of identifying oneself through user/counter-

password, indicates that the simile with the biometric fingerprint is that it allows a more

stronger than the simple username/password pair, since biometric data is more complex.

jos to reproduce and break than a password. For that reason, they indicated that it is treated as

if it were a password, since with the fingerprint "no other employee can supplant the

identity of others in a simple way. In this case, the user is the employee ID and the

password is the template of your fingerprint".

5) Other questions that they consider clarifying or convenient for the system that, according to

can searches for the correspondence of the biometric data provided by the employee when

proceeds to the action of signing, with the way in which the registration of the data is produced, prior

confrontation and coincidence that it manifests is of the "authentication" type.

It states that the biometric validation system has as its sole objective and purpose the

unequivocal identification of an employee within the system providing guarantees to the same

in the face of any attempt to impersonate their identity, making it difficult to reproduce the

footprint by a third party.

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

"INITIATE PUNISHMENT PROCEDURE against MARTORELL LOGISTICS SERVICES

SIGLO XXI, S.L., with CIF B65050247, for the alleged infringement of article 35 of the RGPD

in accordance with article 83.4 a) of the RGPD."

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

Common nistrative of the Public Administrations, the sanction that could correspond se-

administrative fine of 20,000 euros, without prejudice to what results from the investigation."

SIXTH: The respondent makes the following allegations:

1) Uses a minutiae-based fingerprint pattern, a limited number are identified

of footprint shapes and their position within it, associating an algorithm. The boss

is stored encrypted, containing the position and type of minutiae, not being possible to "apply"

Reverse engineer templates to retrieve fingerprint images.

2) "A fingerprint reader is used that reads the employee's fingerprint for the first time and creates the

dot pattern, but it does not save the fingerprint image as such, but rather an algorithm derived

do of the points obtained in the pattern. When a worker puts his finger to clock in

the recorder, the reader reads the points and compares them with the database in which they are found.

finds the algorithm, which has also been stored in encrypted form; what converts it

in a unique alphanumeric code associated with the pattern of the fingerprint read for the first time. That

the device reads the fingerprint and compares it against an encrypted pattern is exactly the same

identification process in a password or smart card, so by not storing

the image of the fingerprint and make the identification by means of a code, we understand that it is not

We would be talking about biometric data in accordance with the definition of article 4.14 RGPD."

3) "The system used cannot always identify the person without ambiguity, unlike

evidence of what would happen if, for example, genetic data that is unique were used. And it,

since the identification in the group of workers is done with coordinates that

are not unique in the world, therefore, the identification of the employee is done without using the

biometric data, that is, the fingerprint. In conclusion, the footprint pattern does not meet the requirement

site of uniqueness." Therefore, the employee's fingerprint pattern is not biometric data.

in accordance with article 4.14 of the RGPD, therefore, it is not appropriate to apply article 9 of the

RGPD as a special category of data in terms of the purpose of data processing

biometric"

4) The attendance and working hours control system, to implement the system through

your presence management software called ***PROGRAMA.1 was contracted with the company

sa TECISA 74, S.L. and the installation of the recorders (***FICHADORAS.1) that contain the

fingerprint readers (***READER.1) at access to work areas. TECISA uses the

technology of ***LECTOR.1/IDEMIA in relation to the identification system through

fingerprint.

5) Contracted the services of TECISA 74, S.L. for being a reference provider for the Administration

Public transfer, as evidenced on the provider's own website

***URL.1, from which it follows that “the Spanish Ministry of Justice (National Court)

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

9/25

National), the General Secretariat of Penitentiary Institutions of the Ministry of the Interior of Es-

Spain, the Ministry of Employment and Social Security in the Control of access of inmates in the

Temporary Stay Centers for Immigrants of Ceuta and Melilla, Getafe City Council

and the Community of Madrid in its Campus for Justice have trusted TECISA 74, S.L.

as a provider of access and presence control services.” Furthermore, in the same

website, specifically in the section https://www.tecisa.com/quienes-somos, it is reported that

“TECISA 74, S.L. is considered by the Spanish Public Administration as the company

manufacturer of the best software and terminals for access control and labor presence, according to

It is indicated in the recent resolution of the State Heritage Catalog competition, a

Once evaluated, for months, all the proposals presented by more than 100 companies

yes. Among the 195 products presented by national and international companies,

the access control and labor presence terminals manufactured by Tecisa have been,

overwhelmingly, the best valued by a group of experts from the Ministry of Finance

and Public Administrations on behalf of the Spanish State.”

The respondent acted in the belief that the information offered by TECISA

Regarding the treatment of fingerprints, it was valid and in accordance with the RGPD. In addition, it has

an ISO 9001/2015 certification of quality management systems, an international standard that

certifies the ability to regularly provide products and services that meet

the requirements of the client and the applicable laws and regulations.

On the other hand, the claimed company has the ISO IEC 27001/2013 certificate, document two,

“As you have implemented and apply an information security management system

that allows the assurance, confidentiality and integrity of data and its systems

that process them, in addition to the risk assessment and application of necessary controls

to mitigate or eliminate them.”

6) States that despite the fact that the legal basis of the treatment could be article 6.1 b) or the

6.1 c), has chosen to request the consent of its employees as indicated in article

6.1 a) and 9.2 a) of the GDPR.

They consider that there is no pressure at the time of giving consent if it is not

provided by the employees, given that the respondent first informed the representation

of the workers of the new system, who in turn informed the employees of the

company and that the vast majority of employees did not refuse to give their consent.

not even some members of ***SECTION.1 that make up the works council

who have presented this claim, nor has any of them revoked their consent.

neither has the treatment been opposed at any time, not even the trade union section

***SECTION.1 informed the workers of their disagreement on the implementation of the system.

7) States that the presence control and the registration of working hours with a fingerprint pattern

as indicated before, they coexisted with the previous system based on the use of the reader

of cards, until the moment it was suspended due to COVID-19, on 03/14/2020

The own claimant union section of ***SECTION.1, recognizes the existence of the two

systems thus appearing in the start-up agreement.

During the testing phase of the new attendance and working hours control system that

has been interrupted, it is important that there are employees who have used only

ca and exclusively of your card according to the previous face-to-face control, not using the

fingerprint readers according to the new system because the

two systems.

For the total transfers of each month and the reference days, the new transfer system was

used by 40 or 50% of the staff and not all of them.

The action of the Labor and Safety Inspectorate was already provided in previous actions

Social that analyzing the fingerprint face-to-face control system did not find any irregularity

authority, the opposite of what the AEPD states.

It adds that there is no specific instruction or circular on the processing of data through

instead of biometric devices for presence control, which have acted in good faith

in the belief that the control and working day system was in accordance with the RGPD.

They carried out an audit for the 27001/2013 certification of 2019, in which

an evaluation and corresponding analysis of the application ***PROGRAM.1.

8) However, and what has motivated the initial agreement, they have carried out an evaluation

of impact applying the criterion of the Agency that a treatment is being carried out

biometric data for identification purposes, also modifying the record of activities

life of the treatment, and they provide document 3 with the evaluation of the impact and document 4

with the record of modified treatment activity.

They indicate that the impact assessment has been carried out, despite the fact that the control system of

presence and working hours by fingerprint pattern was only valid from the

01/16/2020 to 03/14/2020, that is, it has been inoperative since before the start transfer

of the transfer. It considers that it has been fulfilling and observing required obligations and

requests that it be warned or, where appropriate, reduced to a minimum sanction, also considering that previously analyzed in the risk analysis the assessment of whether or not it proceeded to realization of the Impact Assessment.

9) Refers to other AEPD files on registration with biometric data in which no The obligation to carry out an impact assessment has been imposed as indicated in article 35 of the RGPD such as PS 7044/2019 against a Community of owners (in In reality, it would be E77044/2019, more than seven thousand files are not reached or assigned. sanctioning parties in one year) in which the proceedings were archived without stating that had an impact assessment, according to the minutes of the owners' meeting that approved the 09/26/2017 the installation of “lathes with fingerprint recognition for access to facilities nes” of a social club with a swimming pool, attached to the house. The resolution indicates that there was another access alternative through a photo ID and the technical system is not detailed. unique collection, storage and storage and if the matchmaking system of data when putting the finger to enter was identification one-one, or one several, and it is expressed that “The legitimacy for the treatment of the fingerprint for the access to the facilities by part of the claimed we must look for it in articles 9 and 6 of the RGPD.” Adding no the prohibition will be applied by virtue of consent, article 9.2.a), being in addition to the in detail, a different assumption from the one evaluated here.

And he points out another similar case such as PS 145 / 2019 to the Ministry of Education and Sports of the Junta de Andalucía, in a similar case, a warning was imposed for infraction of the article 13 without there being any sanction for breach of article 35 of the RGPD.

SIXTH: Of the actions carried out in this procedure and of the documentation in the file, the following have been accredited:

PROVEN FACTS

11/25

1) The defendant dedicates its activity to the transport of assembly and assembly of parts of automobiles, being the company SEAT for which they provide services as the only client with about 520 workers. The company's offices are located within the premises of its client, SEAT. The work center has a total area of more than sixty thousand square meters, providing a graph with the location of the hourly-River.

1) Historically, there were two time attendance control terminals using a card. Duran-te 2017, to replace these card terminals, five fingerprint terminals are installed in each work area of the center, with the same purposes. When the respondent responds to the transfer, 07/9/2020, reported that the card signing methods and the new fingerprint, using both to check that it works correctly before implanting definitely the mark.

2) The defendant certifies having consulted the union representation on 11/13/2017, before use of the fingerprint system and individually to employees, from 01/22/2018, in accordance with the provisions of the Personal Data Protection Law staff 15/99 from 13/12. In pleadings, the respondent indicated that the use of the fingerprint was suspended due to COVID 19, on 03/14/2020, and which was only in force from 01/16/2020 to 03/14/2020.

3) The reasons why the respondent prefers the use of the fingerprint over the card are that avoids cases that have occurred of giving the card between employees to sign for the holder, and that an unequivocal identification of the employee is produced, avoiding impersonation due to the dif-conceal the reproduction of the imprint by a third party.

4) The purpose of the fingerprint registration is the control of hours or shifts, in accordance with

with article 34.9 of the Workers' Statute.

5) The employee fingerprint collection and registration system and its use is divided into

two phases: 1 Data registration, 2 Presence registration operation.

Phase 1: it is carried out by an HR technician who, with the transfer management program of the

***PROGRAMA.1 application of the company TECISA, and through a reader called

***READER.1, picks up the print, captures it so that it identifies a limited number of for-

more of the footprint and its position within it (minutiae) turning them into a template

encrypted fingerprint (encrypted information, between 25 to 80 minutiae-fork points are stored)

cation or where a line ends). The full fingerprint image is not stored. In the

database included in the application associates and stores the fingerprint template with the ID

of the employee, name and surnames, NIF. When recording the data, the remote machines or terminals

five in this case, in a synchronization process associated with the application, stores

These values are included: encrypted template, employee ID, first name and last name.

Phase 2: When an employee wants to register his presence, which he can do at any-

ra of the five terminals or recorders-fingerprint readers ***READER.1-, place your finger on

the recorder that through the built-in reader ***READER.1, performs the same process as

mentioned in phase 1 when the employee was registered in the system. in a way that makes

a capture of the characteristic points of the employee's footprint, this capture is encoded

and it is compared with the encoded template that of each employee is stored in the memory.

memory of each recorder and associated with the employee's ID. If correct- both templates co-

incident- the recorder will send the relevant data of the employee. The imprint is never sent

code or the name, only information relevant to the signing is sent: date, time, ID

of the employee and any defined absence code. This data is what is transmitted

have to the application of ***PROGRAM.1 for further processing.

6) The respondent had the risk analysis document for treatment activities

ment, carried out on 04/08/2019, showing the result of the “low risk” activity, with

result that it was not necessary to carry out a data protection impact assessment

(EIPD).

The defendant indicates that while the two signing systems were in operation, there were em-

employees who have used only and exclusively their card with face-to-face control, and

others about 40 or 50% used the fingerprint.

8) Despite the fact that the fingerprint collection system was no longer used for signing from

03/14/2020, after the initiation agreement, the respondent modified the risk analysis of the activities

nities of treatment, and the record of treatment activity to agree that it is specified

sa impact assessment that it states it has carried out although it was not provided.

FOUNDATIONS OF LAW

I

Biometric data is defined by article 4.14 of the GDPR:

"biometric data": personal data obtained from technical processing

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

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

facial or fingerprint data;

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

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

right to the protection of personal data, defined in its article 4.1 as "all

information about an identified or identifiable natural person ("the data subject"); I know

An identifiable natural person is considered to be any person whose identity can be determined,

directly or indirectly, in particular by means of an identifier, such as a

name, an identification number, location data, an online identifier, or one or

various elements of physical, physiological, genetic, psychic, economic,

cultural or social status of that person.

According to the information provided by the respondent, when entering the fingerprint in the

recorder, considering that each recorder has all the templates stored for all

two employees, so that they sign in the one they want, the same is compared in order that

cross access by registering the beginning or the end. It is estimated that the comparison is not

produces one against one, that of the employee who agrees with his, but with all that is-

are stored, performing a one-to-many comparison function each time it is encountered.

come or go In this case, although the image of the fingerprint is not saved entirely, but some

coordinates, each of them in the form of a template, is able to identify

unequivocally to each employee when confronting the taking of the fingerprint with the rest in the terminal

of the existing ones. The functions contained in the algorithm allow extracting the points

characteristics of the fingerprint for later comparison with an associated database

to the group of users previously stored, being able to identify its holder of

among all the templates, processing personal data based on the

fingerprint processing, uniquely identifying said person.

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

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

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

loss or intrusion into the system etc.

Article 9.1 of the RGPD indicates:

“Treatment of special categories of personal data”

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

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

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

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

sexual orientation of a natural person.

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

novel and highly intrusive identification systems for rights and freedoms

rights of natural persons, the constant concern of this authority of

control has been shared by the rest of the authorities for years, as they show

manifest the Working Document on Biometrics, adopted on 08/01/2003 by the Group of the

29, or the subsequent Opinion 3/2012, on the evolution of biometric technologies,

adopted on 04/27/2012, and which has led the community legislator to include

this data among the special categories of data in the GDPR. In this way, being

prohibited its treatment in general, any exception to said prohibition will be

to be subject to restrictive interpretation.

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

should not be processed, unless processing is permitted in situations

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

Members may establish specific provisions on data protection in order to

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

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

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

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

this Regulation, especially in what refers to the conditions of legality of the

treatment. Exceptions to the general prohibition of

treatment of those special categories of personal data, among other things when the

interested party gives his explicit consent or in the case of specific needs, in

particular when the treatment is carried out within the framework of legitimate activities by

certain associations or foundations whose objective is to allow the exercise of

fundamental liberties. (52) “Likewise, exceptions must be authorized to the prohibition of

treat special categories of personal data when established by the Law of the

Union or of the Member States and provided that the appropriate guarantees are given, in order to

protect personal data and other fundamental rights, when it is in the public interest,

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

legislation on social protection, including pensions and for security purposes,

health surveillance and alert, the prevention or control of communicable diseases and other

serious health threats. (...)”

II

Faced with the initial ban on the processing of biometric data that identifies

univocally to the persons of article 9.1), points out article 9.2 b) and 9.4)

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

following:

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

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

Labor law and security and social protection, to the extent that it is authorized
the law of the Union or of the Member States or a collective agreement in accordance with
Law of the Member States that establishes adequate guarantees of respect for the
fundamental rights and the interests of the interested party;
(…)
4. Member States may maintain or introduce additional conditions, including
limitations, with respect to the treatment of genetic data, biometric data or data
related to health."
The correlation to this mention is found in article 9 of the LOPDGDD, which states:
"one. For the purposes of article 9.2.a) of Regulation (EU) 2016/679, in order to avoid
discriminatory situations, the consent of the affected party alone will not suffice to lift
the prohibition of data processing whose main purpose is to identify their ideology,
union membership, religion, sexual orientation, beliefs, or racial or ethnic origin.
The provisions of the preceding paragraph will not prevent the processing of said data under
of the remaining cases contemplated in article 9.2 of Regulation (EU) 2016/679,
when appropriate."
In this sense, article 88 of the RGPD has established that the Member States can
give, through legislative provisions or collective agreements, establish standards
more specific to guarantee the protection of rights and freedoms in relation to
with the processing of personal data of workers in the workplace, in particular
lar, among others, for the purpose of complying with the obligations established by law or by the
collective agreement, management, planning and organization of work. These standards must
include adequate and specific measures to preserve the human dignity of the interests
sated, as well as their legitimate interests and their fundamental rights, in particular, in
relation to, among others, monitoring systems in the workplace.
According to what is established, the treatment must be necessary for the fulfillment of

legal obligations, considering that the same effects of compliance were satisfied

before the fingerprint system with the use of cards, being the fingerprint preferred by the re-

claimed for a series of issues among which the type of damage was not taken into account.

intrusive cough that are used, the risks and guarantees established.

In the first place, as in any type of treatment that is carried out, it must be

prove the need for data processing through the registration of fingerprints and provide

purpose for complying with the legal obligation to record working hours. Is considered

that there may be alternative systems to the one used that comply with the principles of pro-

proportionality, necessity and minimization in data processing. It is not explained why

the identification system is necessary and preferable to the verification system. To be able to use

this system, in accordance with the parameters established in the RGPD, the companies or organizations

Organizations need to demonstrate high levels of proactive responsibility and design by

Defect of Data Protection from before the treatment, including the fact of being

able to justify that the system used is necessary, provided in each context

in which it is going to be implemented and prove that less intrusive technical measures

go do not exist or would not work.

Opinion 3/2012, on the evolution of biometric technologies, adopted on
04/27/2012, and that has led the community legislator to include this data
among the special categories of data in the RGPD states that: “When analyzing the
proportionality of a proposed biometric system, it is necessary to first consider whether
the system is necessary to respond to the identified need, that is, if it is essential
to meet that need, and not just the most suitable or profitable. a second factor
What needs to be taken into account is the probability that the system will be effective in
respond to the need in question in light of the specific characteristics of the
biometric technology to be used. A third aspect to consider is whether the loss
of resulting intimacy is proportional to the expected benefits. If the benefit is
relatively minor, such as increased comfort or slight savings, then the loss
privacy is not appropriate. The fourth aspect to assess the adequacy of a system
biometric is to consider whether a less intrusive means of privacy would achieve the end
wanted".

Opinion 2/2017 on data processing at work of the WG29 (adopted on
06/8/2017) establishes that "although the use of these technologies can be useful to detect
o prevent the loss of intellectual and material property of the company, improving the
productivity of workers and protecting the personal data that is
commissioned by the data controller, it also poses significant challenges in terms of
privacy and data protection. Therefore, a new evaluation of the
balance between the legitimate interest of the employer to protect his business and the expectation
reasonable privacy of the interested parties: the workers”.

For this reason, “Regardless of the legal basis of said treatment, before its start
A proportionality test must be performed in order to determine whether the treatment
is necessary to achieve a legitimate purpose, as well as the measures that must be taken to
guarantee that violations of the rights to privacy and secrecy of

Communications are kept to a minimum. This may be part of an assessment of

impact on data protection (EIPD)".

Before implementing a fingerprint recognition system, the person in charge must

to assess whether there is another less intrusive system with which the same purpose is obtained. The

section 72 of CEPD Guide 3/2019 "on processing of personal data through video

devices", establishes in this sense that: "The use of biometric data and in particular facial

re cognition entail heightened risks for data subjects' rights. It is crucial that recourse to

such technologies takes place with due respect to the principles of lawfulness, necessity,

proportionality and data minimization as set forth in the GDPR. Whereas the use of these

technologies can be perceived as particularly effective, controllers should first of all assess

the impact on fundamental rights and freedoms and consider less intrusive means to

achieve their legitimate purpose of processing".

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

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

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

proportionality and minimization of the data established in the RGPD. Considering that

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

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

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

The translation is from the AEPD).

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

those established in article 6.1 of the RGPD, would be that of express consent. It has not been provided the informative clause that includes the wording of the terms of the collection of such express consent. He adds that there are two others, the fulfillment of an obligation legal tion, 6.1.c) of the RGPD and maintenance of compliance with the contractual relationship, 6.1 b) although the obligation does not derive from the contract but from a norm. So, for example, in the employment context, the treatment of information on salary and benefits derives from the contract. details of the bank account so that the salary can be paid, so that there is a direct and objective link between the processing of the data and the purpose of the execution of the contract. The registration of the fingerprint for the fulfillment of the registration obligation working hours as proposed by the complainant, if the prerequisites are met, it is not necessary necessary for the execution of the contract but in his case it would be for the fulfillment of a legal obligation that must be adapted to the general principles of data processing, after overcoming the prohibition of treatment for the causes assessed in article 9 GDPR

Notwithstanding what has been said, consent within an employment relationship is a legal basis. Exceptional Moaner for:

-The very definition of consent, "any manifestation of free will, specific, informed and unequivocal by which the interested party accepts, either by means of a declaration or a clear affirmative action, the processing of personal data that concerns you" is not part of a balanced position in the relationship. As the GT29 has underlined in various opinions, consent can only be valid if the interested party can actually choose and there is no risk of deception, intimidation, coercion, or material negative consequences. costs (for example, substantial additional costs) if you do not give your consent. The con- feeling will not be free in those cases where there is an element of compulsion, pressure or inability to exercise free will.

-The fact that it can be withdrawn whenever the owner wishes, an element that must be included.

include in the clause before it is provided, provided that the withdrawal of consent

will not entail any cost for the interested party and, therefore, no disadvantage for those who

nes withdraw consent.

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

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

consent) the interested parties have the right to delete the data when the consent

feeling has been withdrawn.

III

The respondent was charged with processing personal data of a special category, and

There is an obligation to have an Impact Assessment on the Protection of the

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

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

ologies, by its nature, scope, context or purposes, entails a high risk for the rights

rights and freedoms of natural persons, the person responsible for the treatment will carry out, before

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

tion of personal data. A single assessment may address a number of operations

similar treatment options that carry similar high risks.

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

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

of data.

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

tado 1 will be required in particular in case of:

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

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

basis decisions are made that produce legal effects for natural persons or that

significantly affect them in a similar way;

b) large-scale treatment of the special categories of data referred to in art.

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

referred to in article 10, or

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

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

of treatment that require an impact assessment related to data protection

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

tea referred to in article 68.

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

treatment that do not require impact assessments related to data protection.

The control authority shall communicate these lists to the Committee.

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

competent control will apply the coherence mechanism contemplated in article 63 if those

Lists include processing activities that are related to the supply of goods or

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

two members, or treatment activities that may substantially affect the free

circulation of personal data in the Union.

7. The evaluation must include at least:

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

of the treatment, including, when appropriate, the legitimate interest pursued by the controller.

ble of the treatment;

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

to with respect to its purpose;

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

refers to paragraph 1, and

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

authority and mechanisms that guarantee the protection of personal data, and to demonstrate the

accordance with this Regulation, taking into account the legal rights and interests

rights of the interested parties and other affected persons.

8. Compliance with the approved codes of conduct referred to in article 40

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

assess the repercussions of the processing operations carried out by said respon-

responsible or in charge, in particular for the purposes of impact assessment relating to the pro-

data tection.

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

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

public or commercial interests or the security of processing operations.

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

has its legal basis in Union law or in the law of the Member State that

applies to the data controller, such Law regulates the specific operation of

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

data protection impact assessment as part of an overall impact assessment

general in the context of the adoption of said legal basis, paragraphs 1 to 7 shall not apply.

application except if the Member States consider it necessary to carry out such an evaluation.

prior to treatment activities.

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

data protection impact assessment, at least when there is a change

of the risk represented by the processing operations."

In development of paragraph 4, the director of the AEPD as a non-exhaustive list, the Directorate

AEP published an indicative list of types of treatment that require an evaluation

impact assessment relating to data protection, indicating: "At the time of analysis

When processing data, it will be necessary to carry out an EIPD in most cases in

which said treatment meets two or more criteria from the list set forth below-

treatment, unless the treatment is on the list of treatments that do not require

EIPD referred to in article 35.5 of the RGPD."

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

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

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

or financial solvency or deduce information about people related to

special categories of data.

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

uniquely qualify a natural person.

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

"accountability" supposes the taking of own responsibility for what is done with the data.

personal data and how the principles are complied with, incorporating appropriate measures and

records to be able to demonstrate compliance. Organizations must

show that they are complying with the standard, including documentation measures on

how the data is processed, for what purpose, until when, and document the processing

methods and procedures to focus the question from an early moment of the construction.

construction of the treatment system. Its implementation enables the minimization of risks

at the time of processing the data, taking into account the proportionality of the data,

the amount of data, etc. Within the EIPD, the guarantees of the rights that

are affected, the analysis of how the right is affected, so that before pro-

give in to the treatment, there is a document that guarantees the subsequent management, help-

to identify and minimize the risks of a data processing project that will require

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

claimed, given the specific form of treatment the nature of the context and the purposes

sites.

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

a budget to which the rest of the legal requirements for the treatment must be added,

legitimate basis and respect for the fundamental principles of data processing pre-

seen in article 5 of the RGPD.

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

two, there is no evidence of carrying out the protection impact assessment of

data.

IV

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

will be sanctioned, in accordance with section 2, with administrative fines of 10,000,000

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

as a maximum of the global total annual turnover of the previous financial year,

opting for the highest amount:

the obligations of the person in charge and the person in charge in accordance with articles 8, 11, 25 to

39, 42 and 43;”

The LOPDGDD establishes in its article 73.t):

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

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

substantial portion of the items mentioned therein and, in particular, the following:

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

pact of the treatment operations in the protection of personal data in the sub-

positions in which it is required.”

v

Article 58.2 of the RGPD 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

processing comply with the provisions of this Regulation, where appropriate, in a

certain manner and within a specified period;

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

the measures mentioned in this section, according to the circumstances of each case

particular;"

SAW

The determination of the sanction that should be imposed for the infraction of article 35 of the RGPD in the present case requires observing the provisions of articles 83.1 and 2 of the RGPD, precepts that, respectively, provide the following:

"one. Each control authority will guarantee that the imposition of administrative fines in accordance with this article for the infringements of this Regulation indicated in sections 4, 9 and 6 are in each individual case effective, proportionate and dissuasive. laugh."

"two. Administrative fines will be imposed, depending on the circumstances of each individual case, in addition to or as a substitute for the measures referred to in article 58, section 2, letters a) to h) and j). When deciding to impose an administrative fine and its amount in each individual case shall be duly taken into account:

the intentionality or negligence in the infringement;

any measure taken by the person responsible or in charge of the treatment to alleviate the nature, seriousness and duration of the offence, taking into account the nature,

to)

scope or purpose of the treatment operation in question, as well as the number of affected parties and the level of damages they have suffered;

b)

c)

the damages suffered by the interested parties;

d) the degree of responsibility of the person in charge or of the person in charge of the treatment, account of the technical or organizational measures that have been applied by virtue of the articles the 25 and 32;

and)

F)

fraction and mitigate the possible adverse effects of the infringement;

any prior infringement committed by the controller or processor;

the degree of cooperation with the supervisory authority in order to remedy the in-

to)

the categories of personal data affected by the breach;

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

b)

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

c)

when the measures indicated in article 58, paragraph 2, have been ordered

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

As a matter of course, compliance with said measures;

d)

cation approved under article 42, and

and)

any other aggravating or mitigating factor applicable to the circumstances of the case,

such as financial benefits obtained or losses avoided, directly or indirectly.

you, through the infraction."

adherence to codes of conduct under article 40 or certification mechanisms

Within this section, the LOPDGDD contemplates in its article 76, entitled "Sanctions and

corrective measures":

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

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

section 2 of the aforementioned article.

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

may be taken into account:

a) The continuing nature of the offence.

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

personal.

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

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

infringement.

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

tion, which cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

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

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

mechanisms for alternative conflict resolution, in those cases in which there are

controversies between them and any interested party.

3. It will be possible, complementary or alternatively, the adoption, when appropriate, of the

remaining corrective measures referred to in article 83.2 of the Regulation (EU)

2016/679."

For the assessment of the sanction, the following aggravating factors are contemplated:

-The nature, seriousness and duration of the infraction, taking into account the nature, al-

scope or purpose of the treatment operation that affects the entire workforce, about 500

employees; (83.2.a RGPD), although the claimed one indicates that not everyone made use of the

fingerprint. The use of the system does not reach two months (01/16 to 03/14/2020, although it was discovered

noce if it is still used.)

-A lack of diligence is included, since the implementation of the system was prepared ahead of time.

ma and did not foresee the impact of the implemented system (83.2.b GDPR, 83.2.d) GDPR). It has not been

provided the impact assessment document that declares it was carried out.

On the other hand, it is observed that it concurs as a mitigating factor that the claimed

is an entity in the logistics sector in which its employees' data is processed, although it does not

concurs “b) The link between the activity of the offender and the performance of treatments

of personal data. (76.2.b LOPDGDD).

As a consequence, the sanction is quantified at 20,000 euros.

On the reasons alleged by the respondent that she contracted with a Spanish company

recognized that provides access control software and terminals in its activity of

“development, installation and maintenance of access control systems, presence la-

labor and security systems” that also has ISO certificates (ENAC) and she

itself has another certificate, it should be noted that the prohibition of

data with exceptions and a treatment designed from the caution of the type was not carried out

of data that were treated, offering guarantees, elements that are not related to the

imputed infraction, not being possible for this reason to reduce the amount proposed.

In view of the foregoing, the following is issued:

MOTION FOR A RESOLUTION

That the Director of the Spanish Data Protection Agency sanction

SERVICIOS LOGÍSTICOS MARTORELL SIGLO XXI, S.L., with CIF B65050247, for a

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

a fine of 20,000 euros.

Likewise, in accordance with the provisions of article 85.2 of the LPACAP,

informs that you may, at any time prior to the resolution of this

procedure, carry out the voluntary payment of the proposed sanction, which will entail

a reduction of 20% of the amount of the same. With the application of this reduction, the

sanction would be established at 16,000 euros, and its payment will imply the termination of the

process. The effectiveness of this reduction will be conditioned to the withdrawal or

Waiver of any administrative action or recourse against the sanction.

In case you chose to proceed with the voluntary payment of the amount specified

above, in accordance with the provisions of article 85.2 cited, must make it effective

by depositing it in the restricted account number ES00 0000 0000 0000 0000 0000 open to

name of the Spanish Agency for Data Protection in the bank

CAIXABANK, S.A., indicating in the concept the reference number of the procedure

that appears in the heading of this document and the cause, by voluntary payment, of

reduction in the amount of the penalty. Likewise, you must send proof of admission to the

Subdirectorate General for Inspection to proceed to close the file.

By virtue thereof, you are notified of the foregoing, and the procedure is made clear to you.

so that within TEN DAYS he can allege whatever he considers in his defense and

present the documents and information that it considers pertinent, in accordance with the

article 89.2 of the LPACAP).

Angel Carralero Fernandez

INSPECTOR/INSTRUCTOR

>>

926-280721

SECOND: On October 19, 2021, the claimed party has proceeded to pay

of the sanction in the amount of 16,000 euros making use of the reduction foreseen in

the motion for a resolution transcribed above.

THIRD: The payment made entails the waiver of any action or resource in via against the sanction, in relation to the facts referred to in the resolution proposal.

FOUNDATIONS OF LAW

I

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of control, and as established in art. 47 of the Organic Law 3/2018, of 5 December, of Protection of Personal Data and guarantee of digital rights (in hereinafter LOPDGDD), the Director of the Spanish Agency for Data Protection is competent to sanction the infractions that are committed against said Regulation; infractions of article 48 of Law 9/2014, of May 9, General Telecommunications (hereinafter LGT), in accordance with the provisions of the article 84.3 of the LGT, and the infractions typified in articles 38.3 c), d) and i) and 38.4 d), g) and h) of Law 34/2002, of July 11, on services of the society of the information and electronic commerce (hereinafter LSSI), as provided in article 43.1 of said Law.

II

Article 85 of Law 39/2015, of October 1, on Administrative Procedure Common to Public Administrations (hereinafter LPACAP), under the rubric "Termination in sanctioning procedures" provides the following:

"one. Started a sanctioning procedure, if the offender acknowledges his responsibility,

the procedure may be resolved with the imposition of the appropriate sanction.

2. When the sanction is solely pecuniary in nature or it is possible to impose a

pecuniary sanction and another of a non-pecuniary nature, but the

inadmissibility of the second, the voluntary payment by the alleged perpetrator, in

any time prior to the resolution, will imply the termination of the procedure,

except in relation to the replacement of the altered situation or the determination of the

compensation for damages caused by the commission of the infringement.

3. In both cases, when the sanction is solely pecuniary in nature, the

competent body to resolve the procedure will apply reductions of, at least,

20% of the amount of the proposed sanction, these being cumulative with each other.

The aforementioned reductions must be determined in the notification of initiation

of the procedure and its effectiveness will be conditioned to the withdrawal or resignation of

any administrative action or recourse against the sanction.

The reduction percentage provided for in this section may be increased

regulations."

In accordance with the above, the Director of the Spanish Agency for the Protection of

Data

RESOLVES:

FIRST: TO DECLARE the termination of procedure PS/00050/2021, of

in accordance with the provisions of article 85 of the LPACAP.

SECOND: NOTIFY this resolution to LOGISTICS SERVICES

MARTORELL SIGLO XXI, S.L.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure as prescribed by

the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure

Common of the Public Administrations, the interested parties may file an appeal

contentious-administrative before the Contentious-administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the

Contentious-Administrative Jurisdiction, within a period of two months from the

day following the notification of this act, as provided in article 46.1 of the

aforementioned Law.

Sea Spain Marti

Director of the AEPD, P.O. the Deputy Director General for Data Inspection, Olga

Pérez Sanjuán, Resolution 4/10/2021

968-160721