Procedure No.: PS/00127/2020

 RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: The claim filed by Ms. A.A.A. (hereinafter the claimant),

has entry dated 04/29/2019 in the Spanish Agency for Data Protection.

The claim is directed against IBERIA LÍNEAS AÉREAS DE ESPAÑA, S.A.

UNIPERSONAL OPERATOR, with NIF A85850394 (hereinafter, the claimed). The

reasons on which the claim is based are: that on 01/24/2019 the C.G.T (Confederation

Labor Department) asked the company to follow a series of guidelines: creation and

notification of the mandatory file and obligation to duly inform the

workers before the collection of fingerprints from service agents

auxiliaries for a new signing system that would be implemented in the near future. The

02/27/2019 Iberia answers that it is a lawful and adequate treatment, in addition

measures for safe treatment. However, to date there has been no

provided no document to the workers who register their fingerprint.

SECOND: The General Subdirectorate for Data Inspection proceeded to transfer the

the claim to the respondent to report on the facts and measures

taken, having knowledge of the following extremes:

On 06/18/2019, the claim submitted for analysis was transferred to the respondent

of the decision taken in this regard. Likewise, he was required so that within the term of

one month send certain information to the Agency:

- Copy of the communications, of the adopted decision that has been sent to the

claimant regarding the transfer of this claim, and proof that

the claimant has received communication of that decision.

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

claim.

- Report on the measures adopted to prevent the occurrence of

similar incidents.

- Any other that you consider relevant, etc.

On 07/19/20196 the respondent responded to the request for information

answering the questions raised and providing the following documentation:

- Letter from the CGT dated 01/24/2019.

- Response from IBERIA of 01/29/2019.

- CGT letter of 03/18/2019.

- Analysis of the impact on privacy of the treatment in question.

- Communication to all employees on 05/25/2018.

- Privacy policy for IBERIA employees.

- Screenshots of the Intranet and the app for employees of the

business.

Subsequently, on 09/12/2019, the respondent was asked to provide the study of

Impact evaluation; responding the next day stating that the aforementioned

report could only be provided in MS Excel format, not having been accepted as

valid in the electronic headquarters, reason why he proceeded to present it through the

Agency physical record.

THIRD: On 10/09/2019, in accordance with article 65 of the LOPDGDD, the

Director of the Spanish Agency for Data Protection agreed to admit for processing the

claim filed.

FOURTH: On 09/30/2020, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged

infringement of article 13 of the RGPD, sanctioned in accordance with the provisions of article

58.2.b) of the RGPD.

FIFTH: Once the initiation agreement was notified, the claimant on 10/15/2010 submitted

brief of allegations stating in summary the following: that it was reiterated in the

allegations made in writing on 07/19/2019 and stated that it had been

prepared and communicated to the staff informative note on biometric processing

using fingerprint recognition or facial recognition systems

for access control.

SIXTH: On 10/21/2020, a period of practice tests began,

remembering the following

- Consider reproduced for evidentiary purposes the claim filed by the

claimant and his documentation, the documents obtained and generated by the

Inspection Services that are part of file E/05886/2019.

- Consider reproduced for evidentiary purposes, the allegations to the agreement of

home filed by the respondent and the documentation that accompanies them.

SEVENTH: On 02/26/2020, a Resolution Proposal was issued in the sense that

by the Director of the AEPD, the person claimed for infraction of article 13 will be sanctioned

of the RGPD, typified in article 83.5.a) of the RGPD, with warning of

in accordance with article 58.2.b) of the RGPD.

After the term legally indicated at the time of this Resolution, the

The respondent had not submitted any allegation brief.

EIGHTH: Of the actions carried out in this proceeding, they have been

accredited the following:

PROVEN FACTS

FIRST: The claimant submitted an entry document dated 04/29/2019 in the

Spanish Agency for Data Protection, stating that on 01/24/2019 C.G.T

(General Labor Confederation) asked the company for information on the

implementation of the access system and to follow a series of guidelines on the

same: creation and modification of the mandatory file and obligation to inform

duly to the workers before the collection of the fingerprints of the

auxiliary service agents for a new signing system that will be implemented in

a near future; on 02/27/2019 the respondent indicated that it was a lawful treatment,

adequate and safe; without any document being provided to the workers

registering your fingerprint.

SECOND: There is a letter from the CGT dated 01/24/2019 expressing its

non-conformity with the guidelines followed by the respondent before the collection of fingerprints

fingerprints for the implementation of our system of signing in the company, without

at no time had the workers been duly informed of the

creation and notification of the mandatory file.

THIRD: The respondent's response is recorded stating that the substitution of the

magnetic cards by the use of the fingerprint limited exclusively to the area of

airport ramp and the workers who work there implies lawful treatment

protected in the public interest of the claimed, adequate and secure data

sensitive personnel involved; that the respondent has already been informed of this type of

treatment within its privacy policy available from May 2018 to

over the internet.

FOURTH: On 03/18/2019 CGT indicated that the information provided by the company

to inform his workers was quite scarce from what he understood to be

insufficient despite being said to respond to appropriate treatment and

needs of it.

FIFTH: On 09/13/2019 the respondent provided an Impact Assessment of the treatment

carried out on the treatment of fingerprints for access control.

SIXTH: On 10/15/2020 the respondent has provided informative communication

supplementary to employees Informative Note on data processing

biometrics through fingerprint recognition systems or

Facial recognition for access control.

FOUNDATIONS OF LAW

The Director of the Agency is competent to resolve this procedure.

Spanish Data Protection, in accordance with the provisions of art. 58.2 of the

RGPD and in the art. 47 and 48.1 of LOPDGDD.

Yo

The legitimacy for the treatment of the fingerprint for the control of the

workers by the employer we must look for it in articles 9 and 6 of the RGPD.

II

Article 9 of the RGPD establishes in its sections 1 and 2.b) the following:

"1. The processing of personal data that reveals the origin

racial or ethnic origin, political opinions, religious or philosophical convictions, or

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

uniquely identify a natural person, data related to health or data

relating to the sexual life or sexual orientations of a natural person.

2. Section 1 will not apply when one of the

following circumstances:

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 in the field of labor law and safety and protection

social, to the extent authorized by the Law of the Union of the

Member States or a collective agreement under the law of the

Member States that establishes adequate guarantees of respect for the

fundamental rights and the interests of the interested party."

Article 6.1.b) of the RGPD indicates:

"1. The treatment will only be lawful if at least one of the following is met

conditions:

(…)

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

interested party is a party or for the application at the request of the latter of measures

pre-contractual."

The defendant has legitimacy, based on the aforementioned regulations, to

carry out the labor control of its workers and provided that it meets the requirements

indicated in the fifth Legal Basis.

The facts that motivate the claim presented and that are the subject of the present procedure materialize in the request made by the claimant to the claimed in relation to the implementation of a new access system and the obligation to duly inform workers.

III

The claimed facts suppose the violation of what is stated in article 13 of the RGPD, by not duly informing of the planned treatment in relation to the control of signing by fingerprint, in accordance with the pronouncements established in said article.

This article determines the information that must be provided to the interested party in the time of collecting your data, establishing the following:

“Article 13. Information that must be provided when personal data is obtain from the interested party.

1. When personal data relating to him is obtained from an interested party, the responsible for the treatment, at the time these are obtained, will provide all the information indicated below:

a) the identity and contact details of the person in charge and, where appropriate, of their representative;

b) the contact details of the data protection delegate, if any;

c) the purposes of the treatment to which the personal data is destined and the basis legal treatment;

d) when the treatment is based on article 6, paragraph 1, letter f), the legitimate interests of the person in charge or of a third party;

e) the recipients or categories of recipients of the personal data,

in your case;

f) where appropriate, the intention of the controller to transfer personal data to a

third country or international organization and the existence or absence of a

adequacy decision of the Commission, or, in the case of transfers

indicated in articles 46 or 47 or article 49, paragraph 1, second paragraph,

reference to adequate or appropriate safeguards and means of obtaining

a copy of these or the fact that they have been loaned.

2. In addition to the information mentioned in section 1, the person responsible for the

treatment will facilitate the interested party, at the moment in which the data is obtained

personal, the following information necessary to guarantee data processing

fair and transparent

a) the period during which the personal data will be kept or, when not

possible, the criteria used to determine this period;

b) the existence of the right to request from the data controller access

to the personal data related to the interested party, and its rectification or deletion, or

the limitation of its treatment, or to oppose the treatment, as well as the

right to data portability;

c) when the treatment is based on article 6, paragraph 1, letter a), or the

Article 9, paragraph 2, letter a), the existence of the right to withdraw the

consent at any time, without affecting the legality of the

treatment based on consent prior to its withdrawal;

d) the right to file a claim with a supervisory authority;

e) if the communication of personal data is a legal or contractual requirement, or

a necessary requirement to sign a contract, and if the interested party is

obliged to provide personal data and is informed of the possible

consequences of not providing such data;

f) the existence of automated decisions, including profiling, to

referred to in article 22, sections 1 and 4, and, at least in such cases,

significant information about the applied logic, as well as the importance and

anticipated consequences of said treatment for the interested party.

3. When the person in charge of the treatment projects the subsequent treatment of

personal data for a purpose other than that for which it was collected,

will provide the interested party, prior to said further treatment, information

for that other purpose and any additional information relevant to the meaning of paragraph 2.

4. The provisions of sections 1, 2 and 3 shall not apply when and in

to the extent that the interested party already has the information.

In the present case, the claimant declares to address the respondent in writing

requesting that the workers be duly informed before the collection of

fingerprints for the implementation of a new time control system, without

to get any response.

IV

However, the documentation provided to the file contains the answer

offered to the claimant, as stated in the second antecedent, stating that

the replacement of the established system by the use of the limited fingerprint

exclusively to the airport ramp area and the workers who work there

they worked implied a lawful, adequate and secure treatment of personal data

involved and that it had informed through its privacy policy to

via the intranet.

In relation to the issues raised in this case, first of all

It should be noted that the implementation of a time control system based on the

fingerprint by the employer, must be informed to the employees of

complete, clear, concise manner and, in addition, the aforementioned information must be completed

with reference both to the legal bases that cover said type of control of

access, as well as the basic information referred to in article 13 of the

GDPR.

In the case examined, although the respondent's response to the written

submitted by the claimant indicating that the system to be implemented was safe and

pertinent, both the information transmitted by the claimed person and the system

used to communicate the access and time control system is not the most

adequate given the quality and specialty of the data requested, being able to

have made a greater effort in its information policy on the

planned treatment, formulating it in a much more detailed and complete way,

as well as responding to certain casuistry such as the cases of workers who

They refused to provide their fingerprint.

However, it should be noted that the entity in the allegations to the resolution of

beginning of the procedure provided a complementary communication addressed to the

employees Informative Note on the processing of biometric data through

fingerprint recognition or facial recognition systems for the

access control, in accordance with the regulations on the protection of

data and, likewise, the mandatory impact assessment related to the

data protection regulated in article 35 of the RGPD, providing the document correspondent.

Secondly, it should be noted that the installation of a control based on the collection and processing of employee fingerprints implies the processing of your personal data since personal data is all information about an identified or identifiable natural person in accordance with article 4.1 of the RGPD.

As for the fingerprint, it is also about data that must be qualified as biometric data and in accordance with article 4.14 of the RGPD have this consideration when they have been "obtained from a technical treatment specific, relating to the physical, physiological or behavioral characteristics of a natural person that allow or confirm the unique identification of said person, such as facial images or fingerprint data.

This means that, in accordance with article 9.1 of the RGPD, in the case present, the specific regime provided for special categories is applied to them of data provided for in article 9 of the RGPD.

In this sense, recital 51 of the RGPD highlights the nature restrictive with which the treatment of this data can be admitted:

"(51) ... Such personal data should not be processed, unless it is allowed their treatment in specific situations contemplated in this Regulation, given that Member States may lay down provisions

specific on data protection in order to adapt the application of the

rules of this Regulation to the fulfillment of a legal obligation or to the

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

data conferred on the data controller. In addition to the requirements

specific to that treatment, the general principles and other

rules of this Regulation, in particular as regards 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 in the

framework of legitimate activities by certain associations or foundations whose

objective is to allow the exercise of fundamental freedoms.

And recital 52 states that

“(52) Likewise, exceptions to the prohibition of treating

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

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

public, in particular the processing of personal data in the field of legislation

employment, legislation on social protection, including pensions and for purposes of

security, supervision and health alert, prevention or control of diseases

communicable diseases and other serious threats to health…”

In accordance with these considerations, the treatment of biometric data of

special categories will require, in addition to the concurrence of one of the bases

legal provisions established in article 6 of the RGPD, any of the exceptions provided

in article 9.2 of the RGPD.

The analysis of the legal basis of legitimacy to carry out this treatment comes

of article 6 of the RGPD, regarding the legality of the treatment, which in its section 1, letter

b) states: "The treatment will be lawful if at least one of the following is met:

conditions: (...) b) the treatment is necessary for the execution of a contract in the

that the interested party is a party or for the application at the request of the latter of measures

pre-contractual (…)".

By virtue of this precept, the treatment would be lawful and would not require the

consent, when the data processing is carried out for the fulfillment of

labor contractual relationships.

On the other hand, and as highlighted in recital 51 of the same RGPD,

to the extent that the biometric data are of a special category in the cases

of biometric identification (art. 9.1 RGPD), it will be necessary that one of the

the exceptions provided for in article 9.2 of the RGPD that would allow lifting the

general prohibition of the treatment of these types of data established in the article

9.1.

At this point, special mention must be made of letter b) of article 9.2 of the

RGPD, according to which the general prohibition of biometric data processing does not

It will apply when "the treatment is necessary for the fulfillment of

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

of the interested party in the field of labor law and social security and protection,

to the extent authorized by the Law of the Union of the Member States or

a collective agreement in accordance with the law of the Member States establishing

adequate guarantees of respect for fundamental rights and the interests of the interested".

In the Spanish legal system, article 20 of the Consolidated Text of the Statute of workers (TE), approved by Royal Legislative Decree 2/2015, of 23 October, provides for the possibility for the employer to adopt surveillance measures and control to verify compliance with the labor obligations of their workers:

"3. The employer may adopt the measures it deems most appropriate monitoring and control to verify compliance by the worker with their obligations and labor duties, keeping in its adoption and application the consideration due to their dignity and taking into account, where appropriate, the real capacity of the workers with disabilities".

The possibility of using data-based systems is undeniable biometrics to carry out access and time control, although it does not seem that it is or should be the only system that can be used: thus the use of cards personal codes, the use of personal codes, the direct visualization of the point of marking, etc., which may constitute, by themselves or in combination with any of the the other available systems, equally effective measures to carry out the control.

In any case, prior to the decision on the start-up of such a control system and taking into account its implications, processing of biometric data aimed at uniquely identifying a natural person, it would be mandatory to carry out an impact assessment regarding the protection of personal data to assess both the legitimacy of the treatment and its proportionality such as the determination of existing risks and the measures to mitigate them in accordance with the provisions of article 35 RGPD.

In the present case, it must be stated that the entity has accredited the

mandatory impact assessment related to data protection regulated in the

article 35 of the RGPD, providing the corresponding document, since the

09/13/2019 presented the document Impact Assessment of the treatment carried out

cape.

v

On the other hand, biometric data is closely linked to a

person, since they can use a certain unique property of an individual

for your identification or authentication.

According to Opinion 3/2012 on the evolution of biometric technologies,

“Biometric data irrevocably changes the relationship between the body and

identity, as they make the features of the human body legible

by machines and are subject to further use.”

In relation to them, the Opinion specifies that different types of

treatments by pointing out that "Biometric data can be processed and stored in

different ways. Sometimes the biometric information captured from a person is

stored and treated raw, which allows the source from which it comes to be recognized without

special knowledge; for example, a photograph of a face, a photograph of a

fingerprint or voice recording. Other times, raw biometric information

captured is treated in such a way that only certain characteristics or traits are extracted and

they are saved as a biometric template.”

The processing of this data is expressly permitted by the RGPD

when the employer has a legal basis, which is usually the

Work contract. In this regard, the STS of July 2, 2007 (Rec. 5017/2003),

that it has understood legitimate the processing of biometric data carried out by the

Administration for the time control of its public employees, without being precise

the prior consent of the workers.

However, the following should be noted:

O The worker must be informed about these treatments.

O The principles of purpose limitation, necessity,

proportionality and minimization of data.

In any case, the treatment must also be adequate, pertinent and not

excessive for that purpose. Therefore, biometric data that is not

necessary for that purpose should be abolished and the creation will not always be justified.

of a biometric database (Opinion 3/2012 of the Art. 29 Working Group).

O Use of biometric templates: Biometric data should be stored

as biometric templates whenever possible. The template must be extracted from

a way that is specific to the biometric system in question and not used

by other controllers of similar systems in order to ensure that

a person can only be identified in biometric systems that have

a legal basis for this operation.

O The biometric system used and the security measures chosen must

ensure that reuse of the biometric data in question is not possible

for another purpose.

O Mechanisms based on encryption technologies should be used in order to

prevent unauthorized reading, copying, modification or deletion of biometric data.

O Biometric systems should be designed in such a way that they can be revoked

the identity bond.

O You should choose to use specific data formats or technologies that

prevent the interconnection of biometric databases and the disclosure of data

not checked.

O Biometric data must be deleted when they are not linked to the

purpose that motivated its treatment and, if possible, should be implemented

automated data deletion mechanisms.

SAW

Article 83.5 b) of the RGPD considers that the infringement of “the rights of

those interested in accordance with articles 12 to 22”, is punishable, in accordance with the

“with fines

section 5 of the aforementioned article 83 of the aforementioned Regulation,

administrative fees of €20,000,000 maximum or, in the case of a company, a

amount equivalent to a maximum of 4% of the total global annual turnover of the

previous financial year, opting for the highest amount.

The LOPDGDD in its article 71, Violations, states that:

“The acts and behaviors referred to in the regulations constitute infractions.

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law.

The LOPDGDD in its article 72 indicates for prescription purposes: "Infringements

considered very serious:

"1. Based on the provisions of article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

suppose a substantial violation of the articles mentioned in that and, in

particularly the following:

(…)

h) The omission of the duty to inform the affected party about the treatment of their

personal data in accordance with the provisions of articles 13 and 14 of the

Regulation (EU) 2016/679 and 12 of this organic law.

(…)"

7th

The sanctioning procedure that concerns us shows that in the installation of

a new fingerprint attendance control system to be implemented had

been carried out without duly informing with all the guarantees that are indicated

in the data protection regulations, specifically in accordance with what is indicated

in article 13 of the RGPD, and may have incurred in the violation of the same.

Therefore, the conduct of the defendant would constitute a violation of the provisions

in article 13 of the RGPD.

On the other hand, the RGPD, without prejudice to the provisions of its article 83,

contemplates the possibility of resorting to the sanction of warning to correct the

processing of personal data that do not meet your expectations.

Likewise, it is contemplated that the resolution issued will establish the measures

that it is appropriate to adopt so that the conduct ceases, the effects of the infraction are corrected that had been committed, the adequacy of the information offered to users to the requirements contemplated in article 13 of the RGPD, as well as the contribution of means accrediting compliance with the requirements.

However, it should be noted that in the allegations to the agreement to start the In this proceeding, the respondent has provided a copy of the communication made to all the workers and that came to complement the information provided with previously Informative Note on the processing of biometric data through fingerprint recognition or facial recognition systems for the access control, in accordance with those indicated in article 13 of the RGPD, by which is not appropriate to urge the adoption of additional measures as it has been accredited that the claimed party has adopted reasonable measures and prevent them from returning to occurrence of incidents such as the one that gave rise to the claim.

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

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE IBERIA LÍNEAS AÉREAS DE ESPAÑA, S.A. OPERATOR, with NIF A85850394, for an infringement of article 13 of the RGPD, typified in the article 83.5 of the RGPD, a sanction of warning.

SECOND: NOTIFY this resolution to IBERIA LÍNEAS AÉREAS DE SPAIN, S.A. OPERATOR, with NIF A85850394.

In accordance with the provisions of article 50 of the LOPDGDD, the This Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the interested parties may optionally file an appeal for reconsideration

before the Director of the Spanish Agency for Data Protection within a period of

month from the day following the notification of this resolution or directly

contentious-administrative appeal before the Contentious-Administrative Chamber of the

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

the fourth additional provision of Law 29/1998, of 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.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the

LPACAP, the firm resolution may be provisionally suspended in administrative proceedings

if the interested party expresses his intention to file a contentious appeal-

through the

Electronic Registration of

administrative. If this is the case, the interested party must formally communicate this

made by writing to the Spanish Agency for Data Protection,

introducing him to

the agency

[https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other

records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. Also

must transfer to the Agency the documentation that proves the effective filing

of the contentious-administrative appeal. If the Agency were not aware of the

filing of the contentious-administrative appeal within two months from the

day following the notification of this resolution, it would end the

precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es