 File No.: EXP202209921

RESOLUTION OF TERMINATION OF THE PROCEDURE FOR PAYMENT

VOLUNTEER

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

to the following

BACKGROUND

FIRST: On February 20, 2023, the Director of the Spanish Agency for

Data Protection agreed to start a sanctioning procedure against ALBERO FORTE

COMPOSITE, S.L. (hereinafter, the claimed party), through the Agreement that

transcribe:

<<

File No.: EXP202209921

AGREEMENT TO START THE SANCTION PROCEDURE

Of the actions carried out by the Spanish Data Protection Agency and in

based on the following

FACTS

FIRST: A.A.A. (hereinafter, the claiming party) dated August 17, 2022

filed a claim with the Spanish Data Protection Agency.

The claim is directed against ALBERO FORTE COMPOSITE, S.L. with NIF

B54620182 (hereinafter, the claimed party).

The reasons on which the claim is based are the following:

The claimant states that the company claimed takes a photograph of the faces of the

employees from a device at the entrance and that this image is used to clock the

entry and exit at the workplace.

He states that he has never been informed of the use of biometric data, he only

they sign a consent to the use of image rights that could be

used and disseminated for publication on its website, social networks,

campaigns, magazines, brochures, corporate advertising and other support materials

necessary for the dissemination and promotion of the claimed company.

Along with the claim document, provide a copy of a document called:

"Consent for the collection and processing of personal data" signed by the

claimant on XX/XX/2022.

Also attach a copy of an access request, dated 05/10/2022.

On 05/16/2022, you are informed that the answer to your request is already available.

access request and that you can proceed to withdraw it.

Provide a copy of the response received, in which it is reported that the category of

data object of treatment are "identifying data".

The claimant considers the response received insufficient and on 05/17/2022, through

email, the claimed company sends you new documentation that does not give

response to the use of biometric data.

They give you a copy of a document on occupational risk prevention, a report on

presence times from XX/XX/2022 and XX/XX/2022, information on the

treatment of the data of your CV, registration of entry of EPIS and your photograph.

The claimant considers that he was not informed of the need to capture the

biometrics of the face, nor is the company that captures and manages the data informed,

nor about the characteristics of the servers where the information is stored.

biometrics or the purpose of the treatment.

Only the photo taken by the recorder is provided, without biometric proportions

and without the signature of the Data Protection Delegate, informing that his

designation to provide the requested personal information.

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

December, Protection of Personal Data and guarantee of digital rights (in

forward LOPDGDD), on September 23, 2022, said

claim to the claimed party, to proceed with its analysis and inform

this Agency within a month, of the actions carried out to adapt to

the requirements set forth in the data protection regulations.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

Public (hereinafter, LPACAP), was collected on September 27, 2022

as stated in the acknowledgment of receipt in the file.

On October 18, 2022, this Agency received a written response from the

entity claimed where it states that the implementation of the registration of working hours, does not

requires the consent of the worker, being a sufficient basis of legitimacy the

Article 34.9 of the Workers' Statute, which establishes the obligation of

companies to carry out said record of the working day on an individual basis for each

worker and that, in accordance with the provisions of article 6.1 c) of the

European Regulation 2016/76 (RGPD), the processing of personal data of

workers derived from the implementation of the record of working hours is necessary for the

compliance with a legal obligation applicable to the data controller, only

purpose of the treatment.

The claimed entity concludes by saying that it is not in any of the

cases that require an impact assessment, in accordance with article 35

of the GDPR.

THIRD: On October 27, 2022, in accordance with article 65 of the

LOPDGDD, the claim presented by the claimant party was admitted for processing.

FUNDAMENTALS OF LAW

Yo

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

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

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

Organic Law 3/2018, of December 5, on the Protection of Personal Data and

guarantee of digital rights (hereinafter, LOPDGDD), is competent to

initiate and resolve this procedure the Director of the Spanish Protection Agency

of data.

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

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

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

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

subsidiary, by the general rules on administrative procedures."

II

Article 35 of the GDPR, establishes in relation to the impact assessment related to

data protection the following:

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

technologies, by their nature, scope, context or purposes, entail a high risk for the rights and freedoms of natural persons, the data controller carry out, before the treatment, an evaluation of the impact of the operations of treatment in the protection of personal data.

A single assessment may address a number of similar processing operations that carry similarly high risks.

2. The person in charge of the treatment will obtain the advice of the delegate of data protection, if appointed, when carrying out the relative impact assessment to data protection.

3. The impact assessment on data protection referred to in the Paragraph 1 will be required in particular in case of:

a) systematic and exhaustive evaluation of personal aspects of natural persons that is based on automated processing, such as profiling, and on on the basis of which decisions are made that produce legal effects for people physical or that significantly affect them in a similar way;

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

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

4. The control authority will establish and publish a list of the types of operations of treatment that require an impact assessment related to the protection of

data in accordance with section 1.

The supervisory authority will communicate these lists to the Committee 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 the protection of data. The supervisory authority will communicate these lists to the Committee.

6. Before adopting the lists referred to in paragraphs 4 and 5, the authority of competent control will apply the consistency mechanism referred to in article 63 if those lists include processing activities that are related to the offer of goods or services to interested parties or with the observation of the behavior of these in several Member States, or processing activities that may affect substantially to the free flow of personal data in the Union.

7. The evaluation must include at least:

a) a systematic description of the planned processing operations and the purposes of the treatment, including, where appropriate, the legitimate interest pursued by the responsible for the treatment;

b) an assessment of the necessity and proportionality of the operations of treatment with respect to its purpose;

c) an assessment of the risks to the rights and freedoms of the data subjects referred to in paragraph 1, and

d) the measures planned to deal with the risks, including guarantees, measures of security and mechanisms that guarantee the protection of personal data, and demonstrate conformity with this Regulation, taking into account the legitimate rights and interests of the data subjects and other affected persons.

8. Compliance with the approved codes of conduct referred to in the article 40 by the corresponding managers or managers will be duly taken into account

into account when assessing the impact of processing operations carried out by

said controllers or processors, in particular for the purposes of impact assessment

regarding data protection.

9. When appropriate, the controller will seek the opinion of the interested parties or their

representatives 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 person responsible for the treatment, such Law regulates the operation

specific treatment or set of operations in question, and has already been

carried out a data protection impact assessment as part of

a general impact assessment in the context of the adoption of that basis

legal, paragraphs 1 to 7 shall not apply unless the Member States

consider it necessary to carry out said evaluation prior to the activities of

treatment.

11. If necessary, the controller will examine whether the processing is in accordance with the

impact assessment relating to data protection, at least where there is a

change in risk posed by processing operations."

II

In this case, the respondent entity states that it does not have an impact assessment

for not being in any of the cases in which the law requires it.

In this sense, it should be noted that the list is based on the criteria established by the

“GUIDELINES ON IMPACT ASSESSMENT RELATING TO THE

DATA PROTECTION (EIPD) AND TO DETERMINE IF THE PROCESSING

“PROBABLY INVOLVES HIGH RISK” FOR PURPOSES OF GDPR”,

adopted on 4/04/2017 and last revised and adopted on 10/4/2017, WP 248

rev.01 of GT 29 that complements them and should be understood as a list not

exhaustive:

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

Refers to article 9.1 of the GDPR, data relating to criminal convictions or offenses to

those referred to in article 10 of the GDPR or data that allows determining the situation

financial or patrimonial solvency or deduce information about the persons related to

nothing with special categories of data.

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

charge uniquely to a natural person.”

9. Data processing of vulnerable subjects…”

In the same Guidelines, it is stated:

“In order to offer a more concrete set of treatment operations that re-

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

particulars of article 35, paragraph 1, and article 35, paragraph 3, letters a) to c), the

list to be adopted at national level under Article 35(4) and the

recitals 71, 75 and 91, and other GDPR references to processing operations

that are “likely to carry a high risk”, the nine criteria should be considered

following:

“7. Data related to vulnerable data subjects (recital 75):

The treatment of this type of data represents a criterion due to the increase in the

balance of power between the interested parties and the data controller, which implies

ca that individuals may be unable to authorize or deny treatment of

your data, or to exercise your rights.

Vulnerable stakeholders may include children (considered not to be ca-

peace to deny or authorize consciously and responsibly the treatment of their

data), employees.

As the registration system is an innovative and very

intrusive to the fundamental rights and freedoms of natural persons, the

GDPR establishes the obligation to manage the risk that for the rights and

freedoms of the people supposes those treatments. This risk arises both from the

the very existence of the treatment, as well as the technical and organizational dimensions

of the same.

The risk arises from the purposes of the processing and its nature, and also from its scope

and the context in which it unfolds.

The complexity of the risk management process has to be adjusted, not the size of the

entity, the availability of resources, its specialty or sector, but rather

possible impact of the processing activity on the interested parties and on the company itself

treatment difficulty.

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

which are contemplated in OPINION 3/2012 ON THE EVOLUTION OF THE

BIOMETRIC TECHNOLOGIES of GT 29 of 04/27/2012:

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

crucial question.

On the one hand, the size of the template must be large enough to manage the

security (avoiding overlaps between the different biometric data, or

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

the risks of reconstruction of biometric data.

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

in large centralized databases, given the potential consequences

harmful to the people affected.

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

and availability with respect to the databases would clearly be detrimental to

any future application based on the information contained in said databases

data, and would also cause irreparable damage to the data subjects.

- The transfer of information contained in the database.

-Security measures must be adopted for data processing

biometrics (storage, transmission, extraction of characteristics and

comparison, etc.) and especially if the data controller transmits such data

via Internet.

Security measures could include, for example, the coding of templates

and protection of encryption keys apart from access control and a

protection that makes data reconstruction virtually impossible

originals from the templates.

-Likewise, the WORKING DOCUMENT ON BIOMETRY, adopted on

08/01/2003, from GT29, believes that biometric systems related to characteristics

physical characteristics that leave no trace or biometric systems related to physical characteristics

that leave a trace but do not depend on the memorization of the data possessed by a

person other than the person concerned (in other words, the data is not stored in the

access control device or central database) create fewer risks

for the protection of the fundamental rights and freedoms of individuals

can distinguish biometric data that is processed centrally from

biometric reference data that is stored on a mobile device and the process

compliance is performed on the card and not on the sensor or when it is part of the

mobile device).

-It is generally accepted that the risk of reusing biometric data obtained

from physical traces left by people inadvertently for purposes

incompatible data is relatively low if the data is not stored in databases.

Centralized data, but in the possession of the person and are inaccessible to third parties.

Centralized storage of biometric data also increases the risk

of the use of biometric data as a key to interconnect different databases, which

which could make it possible to obtain detailed profiles of a person's habits both

public and private level.

In addition, the question of compatibility of purposes leads us to the interoperability of

different systems that use biometrics.

The standardization that interoperability requires can lead to greater

interconnection between databases.

- Obvious risks if the technology used does not sufficiently guarantee that

the template obtained from the biometric data will not match the one used in

other similar systems.

Regarding the guarantees to be implemented that must be contained in the EIPD, the Guide

"Data protection in labor relations" of the AEPD contemplates, by way of

reference ten aspects that can be taken into account.

The claimed party has stated that the EIPD was not carried out because there is no

in any of the cases that require it, according to article 35 of the GDPR.

However, this is not an exhaustive list, but the

complexity of the risk management process, taking into account not the size of the

entity, the availability of resources, its specialty or sector, but the possible

impact of the processing activity on the interested parties and the difficulty of the

treatment.

IV.

The alleged infringement is typified in article 83.4.a) of the GDPR, which indicates:

Violations of the following provisions will be sanctioned, in accordance with the

paragraph 2, with administrative fines of maximum EUR 10,000,000 or,

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

total annual global business volume of the previous financial year, opting for the

of greater amount:

a) The obligations of the controller and the person in charge under articles 8, 11, 25

to 39, 42 and 43;”

The LOPDGDD establishes in its article 73.t):

"Based on what is established in article 83.4 of Regulation (EU) 2016/679,

are considered serious and will prescribe after two years the infractions that suppose a substantial violation of the articles mentioned therein and, in particular, the following:

t) The processing of personal data without having carried out the evaluation of the impact of processing operations in the protection of personal data in the su-posts in which it is enforceable."

V

Pursuant to the provisions of article 58.2 of the GDPR, the Spanish Agency for Data Protection, as a control authority, has a set of corrective powers in the event of an infringement of the precepts of the GDPR.

Article 58.2 of the GDPR provides the following:

"2 Each control authority will have all the following corrective powers in-stated below:

(…)

"d) order the controller or processor that the processing operations compliance with the provisions of this Regulation, where appropriate, in accordance with a certain manner and within a specified period;"

(...)

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

particular case;"

Therefore, based on the foregoing, this Agency considers that

we could find ourselves facing a violation of article 35 of the GDPR, indicated in the

foundation of law II.

Likewise, if the existence of an infringement is confirmed, in accordance with the provisions of

the aforementioned article 58.2.d) of the GDPR, in the resolution the defendant may be ordered to

suspension of treatment until the impact evaluation has been carried out.

SAW

If the infringement is confirmed, in addition to the security measures suggested in the

basis of law III, relating to the coding of the templates, or

establishment of keys to control access, it could be agreed to impose the

responsible for adopting adequate measures to adjust its performance to the

regulations mentioned in this act, in accordance with the provisions of the aforementioned article

58.2 d) of the GDPR, according to which each control authority may “order the

controller or processor that the processing operations are

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

certain manner and within a specified period…”.

The imposition of this measure is compatible with the sanction consisting of a fine

administration, according to the provisions of art. 83.2 of the GDPR.

It is noted that not attending to the possible order to adopt measures imposed by

this body in the sanctioning resolution may be considered as a

administrative offense in accordance with the provisions of the GDPR, classified as

infraction in its article 83.5 and 83.6, being able to motivate such conduct the opening of a

subsequent administrative sanctioning procedure.

Therefore, the Director of the Spanish Data Protection Agency AGREES:

FIRST: INITIATE SANCTION PROCEDURE against ALBERO FORTE

COMPOSITE, S.L., with NIF B54620182, for the alleged violation of article 35 of the

RGPD typified in article 83.4.a) of the RGPD, as a serious infringement, and for the purposes of

prescription in article 73.t) of the LOPDGDD.

SECOND: APPOINT as instructor B.B.B. and, as secretary, to C.C.C.,

indicating that any of them may be challenged, if applicable, in accordance with the

established in articles 23 and 24 of Law 40/2015, of October 1, on the Regime

Legal Department of the Public Sector (LRJSP).

THIRD: INCORPORATE into the disciplinary file, for evidentiary purposes, the

claim filed by the claimant and its documentation, as well as the

documents obtained and generated by the Sub-directorate General of Inspection of

Data in the actions prior to the start of this sanctioning procedure.

FOURTH: THAT for the purposes provided for in art. 64.2 b) of Law 39/2015, of 1

October, of the Common Administrative Procedure of Public Administrations

sanction that could correspond would be €20,000 (twenty thousand euros).

FIFTH: NOTIFY this agreement to ALBERO FORTE COMPOSITE, S.L.,

with NIF B54620182, granting a hearing period of ten business days so that

Formulate the allegations and present the evidence that you consider appropriate. In its

pleadings must provide your NIF and the procedure number that appears

at the top of this document.

If, within the stipulated period, he does not make allegations to this initial agreement, the same

may be considered a resolution proposal, as established in article

64.2.f) of Law 39/2015, of October 1, on the Common Administrative Procedure of

Public Administrations (hereinafter, LPACAP).

In accordance with the provisions of article 85 of the LPACAP, you may recognize your

responsibility within the period granted for the formulation of allegations to the

present initiation agreement; which will entail a reduction of 20% of the

sanction that should be imposed in this proceeding. With the application of this

reduction, the sanction would be established at 16,000 euros, resolving the

procedure with the imposition of this sanction.

In the same way, it may, at any time prior to the resolution of this

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

will mean a reduction of 20% of its amount. With the application of this reduction,

the sanction would be established at [Enter the corresponding text 16,000 euros and

Your payment will imply the termination of the procedure, without prejudice to the imposition of

the corresponding measures.

The reduction for the voluntary payment of the penalty is cumulative to the corresponding

apply for acknowledgment of responsibility, provided that this acknowledgment

of the responsibility is revealed within the period granted to formulate

allegations at the opening of the procedure. Voluntary payment of the referred amount

in the previous paragraph may be done at any time prior to the resolution. In

In this case, if both reductions were to be applied, the amount of the penalty would remain

established at 12,000 euros.

In any case, the effectiveness of any of the two aforementioned reductions will be

conditioned to the withdrawal or resignation of any action or appeal via

administrative against the sanction.

C / Jorge Juan, 6

28001 – Madrid

In the event that you choose to proceed with the voluntary payment of any of the amounts previously indicated 16,000 or 12,000 euros, you must make it effective through your Payment to account IBAN number: ES00-0000-0000-0000-0000-0000 (BIC/SWIFT Code: CAIXESBBXXX) opened on behalf of the Spanish Data Protection Agency in the banking entity CAIXABANK, S.A., indicating in the concept the number of reference of the procedure that appears in the heading of this document and the cause of reduction of the amount to which it receives.

Likewise, you must send proof of income to the General Subdirectorate of Inspection to continue with the procedure in accordance with the quantity entered.

The procedure will have a maximum duration of nine months from the date of the initiation agreement or, where appropriate, of the draft initiation agreement. After this period, its expiration will occur and, consequently, the file of performances; in accordance with the provisions of article 64 of the LOPDGDD.

In compliance with articles 14, 41 and 43 of the LPACAP, it is noted that, as regards successively, the notifications that are sent to you will be made exclusively in a electronically, through the Unique Authorized Electronic Address (dehu.redsara.es) and the Electronic Notification Service (notifications.060.es), and that, if you do not access their rejection will be recorded in the file, considering the process completed and following the procedure. You are informed that you can identify before this Agency an email address to receive the notice of making available to the notifications and that failure to practice this notice will not prevent the notification be considered fully valid.

Finally, it is noted that in accordance with the provisions of article 112.1 of the

LPACAP, there is no administrative appeal against this act.

Mar Spain Marti

Director of the Spanish Data Protection Agency

935-121222

>>

SECOND: On February 28, 2023, the claimed party has proceeded to pay

of the penalty in the amount of 12,000 euros making use of the two reductions

provided for in the initiation Agreement transcribed above, which implies the

recognition of responsibility.

THIRD: The payment made, within the period granted to formulate allegations to

the opening of the procedure, entails the waiver of any action or appeal via

against the sanction and acknowledgment of responsibility in relation to

the facts referred to in the Commencement Agreement.

FOURTH: In the previously transcribed initiation agreement, it was indicated that, if

Once the infringement is confirmed, it could be agreed to impose on the controller the adoption of

adequate measures to adjust its performance to the regulations mentioned in this

act, in accordance with the provisions of the aforementioned article 58.2 d) of the GDPR, according to the

which each control authority may "order the person responsible or in charge of the

processing that the processing operations comply with the provisions of the

this Regulation, where appropriate, in a certain way and within a certain

specified term…". Specifically, it indicated that the resolution could order

the requested suspension of treatment until the evaluation has been carried out

of impact.

Having recognized the responsibility for the infringement, the imposition of

the measures included in the Initiation Agreement.

FUNDAMENTALS OF LAW

Yo

Competence

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

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

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

Organic Law 3/2018, of December 5, on the Protection of Personal Data and

guarantee of digital rights (hereinafter, LOPDGDD), is competent to

initiate and resolve this procedure the Director of the Spanish Protection Agency

of data.

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

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

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

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

subsidiary, by the general rules on administrative procedures."

II

Termination of the procedure

Article 85 of Law 39/2015, of October 1, on Administrative Procedure

Common for Public Administrations (hereinafter, LPACAP), under the heading

"Termination in disciplinary proceedings" provides the following:

"1. Initiated a disciplinary procedure, if the offender acknowledges his responsibility,

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

2. When the sanction has only a pecuniary 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 presumed perpetrator, in

any moment 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 offence.

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

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

20% of the amount of the proposed penalty, these being cumulative among themselves.

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 resource against the sanction.

The percentage reduction provided for in this section may be increased

according to regulations."

According to what has been stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: DECLARE the termination of procedure EXP202209921, in

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

SECOND: Require in application of articles 90.3 of the LPCAP, and 58. 2.f), of the

GDPR, to ALBERO FORTE COMPOSITE, S.L, so that within ten days,

temporarily or permanently limit the treatment of the facial recognition system

for the purpose of labor control, as long as it does not have an evaluation of the impact of

data protection of the valid treatment, which takes into account the risks for the

rights and freedoms of employees and the appropriate measures and guarantees for their

treatment, or even if it were carried out, it would be necessary to make the consultation forecast that is

established in article 36 of the GDPR.

After the time granted, you must inform this AEPD. The lack of attention to

requirement may lead to the commission of a violation of article 83.6 of the

GDPR.

THIRD: NOTIFY this resolution to ALBERO FORTE COMPOSITE,

S.L.

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

Resolution will be made public once the interested parties have been notified.

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

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

Common of Public Administrations, interested parties may file an appeal

administrative litigation before the Administrative Litigation 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 for in article 46.1 of the

referred Law.

Mar Spain Marti

Director of the Spanish Data Protection Agency

C / Jorge Juan, 6

28001 – Madrid

1259-121222

www.aepd.es

sedeagpd.gob.es