 File No.: EXP202102806

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 May 20, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against ESTUDIOS

EUROPEOS DE POSTGRADO Y EMPRESA, S.L. (hereinafter, the claimed party),

through the Agreement that is transcribed:

<<

File No.: EXP202102806

AGREEMENT TO START A SANCTION PROCEDURE

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

based on the following

FACTS

FIRST: Ms. A.A.A. (hereinafter, the complaining party), on August 9,

2021, filed a claim with the Spanish Data Protection Agency. The

claim is directed against EUROPEAN POSTGRADUATE STUDIES AND BUSINESS,

SL with NIF B86256419 (hereinafter, the claimed party). The reasons on which he bases

the claim are as follows:

The claimant states that, in March 2021, she was hired to replace the tutor

some courses given by the entity CEUPE - EUROPEAN STUDIES OF

POSTGRADUATE AND COMPANY, S.L. To develop this activity they provided him with a

corporate email account. According to him, upon accessing it, he realized

that the email account was not yours, but was the email account of the person to

which it replaced. Instead of giving him a new corporate account, the one from the company was reused.

former worker. Apparently the email account was not configured correctly

since, when sending emails from your email, instead of appearing the name

of the claimant, there was that of the tutor whom she replaced.

On 4/13/21, he communicated the facts by sending an email to the entity

claimed. The same day they replied that the account assigned to him is the

used by the other tutor, being able to eliminate the folders that she considered appropriate.

The claimant states that through the assigned account she could access all

the emails sent and received by the previous worker, including the

tax data and billing to third parties with all your personal data, telephone numbers

address, bank account.

The claimant considers that the entity claimed violated the protection regulations

of data by allowing you to access the aforementioned information, since in it there are data

personal data of the students and of the worker whom he replaced.

The claimant currently does not provide services in the entity claimed and thinks

that the person who replaces you will be able to access your emails as well as

she agreed to those of her predecessor.

Together with the claim, it provides various screen impressions made to the email

controversial email.

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

December, Protection of Personal Data and Guarantee of Digital Rights

(hereinafter LOPDGDD), said claim was transferred 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

(hereinafter, LPACAP), by electronic notification, was received in

dated October 7, 2021, as stated in the certificate in the file.

On November 5, 2021, this Agency received a written response

indicating that the claimant began to work as an employee at CEUPE to replace

sick leave of another worker within the same field and tasks, so the

The complainant's work was the continuation of those specific teaching activities

and tutorials with students, for which knowledge of all the

antecedents and communications given teacher-student and that the data to which the

complainant was able to have access to the students, it was in the exercise of his activity

work and as a necessity for the exercise of their tasks, which were continuity of the

of the teacher-tutor whom she replaced on leave.

It states that the complainant is assigned the enabled email

initially for the operation of online courses and attention to tutorials

assigned and that all training workers, also called "tutors",

have an email account for exclusively professional use that

they are given when they are assigned a group of students to train.

This email account is assigned to this group of students

exclusively and when the tutor changes, the only thing that is done is to unsubscribe

to the previous tutor and registration to the new one, but maintaining this same email account

electronic. This procedure must be like this since the new tutor must be able to

access all the queries of the students who have made the previous tutor. In

In this sense, the emails, as the complainant rightly says, are "corporate" and

property of CEUPE, and therefore they do not belong to any third party, having been used in

at all times for the use and scope of work and activity of the company.

Indicates that the irregularity in its use belongs to the user himself, in this case the

complainant. The data to which the complainant may have accessed as

worker of the company, are those necessary for the exercise of its activity, and between

it is logical for them to know and access the personal data of the students, and equally

to the history of communications in the course of the previous tutor.

Finally, it adds that all access to personal data has been in the

internal and labor of the company, due to the needs of its activity and that there is no

no complaint by the owners of the data, nor prejudice to them, to

which he has been able to access in the exercise of his work.

THIRD: On December 3, 2021, in accordance with article 65 of the

LOPDGDD, the claim filed by the claimant was admitted for processing.

FOUNDATIONS OF LAW

Yo

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

(General Data Protection Regulation, hereinafter RGPD), 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 Agency for

Data Protection.

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

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

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

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures."

II

Previous questions

In the present case, in accordance with the provisions of article 4.1 of the RGPD, it consists

the processing of personal data, since European Studies

de Postgrado y Empresa, S.L., is a commercial company dedicated to training and

teaching that, for the organization, development and delivery of its own studies,

performs personal data processing.

It carries out this activity in its capacity as data controller, since it is

who determines the purposes and means of such activity, by virtue of article 4.7 of the RGPD:

“responsible for the treatment” or “responsible”: the natural or legal person, authority

public, service or other body that, alone or jointly with others, determines the ends and

treatment god; if the law of the Union or of the Member States determines

the purposes and means of the treatment, the person in charge of the treatment or the specific criteria for their appointment may be established by the Law of the Union or of the States.

two members.

Article 4 section 12 of the RGPD defines, in a broad way, the "violations of se-

security of personal data" (hereinafter security breach) as "all

those violations of security that cause the destruction, loss or alteration

accidental or unlawful transfer of personal data transmitted, stored or processed in

otherwise, or unauthorized communication or access to such data."

In the present case, there is a security breach of personal data in the cir-

circumstances indicated above, categorized as a breach of confidentiality, any

time the claimant states that she allegedly had access to the records

complete list of the emails of the employee she replaced, with details of

personal nature that were not necessary for the exercise of their activity.

According to GT29, a "Breach of confidentiality" occurs when there is

unauthorized or accidental disclosure of personal data, or access to

themselves.

It should be noted that the identification of a security breach does not imply the imposition

sanction directly by this Agency, since it is necessary to analyze the

diligence of those responsible and in charge and the security measures applied.

III

Article 5.1.f) of the RGPD

Article 5.1.f) of the RGPD establishes the following:

"Article 5 Principles relating to processing:

1. The personal data will be:

(…)

f) processed in such a way as to ensure adequate security of the data

including protection against unauthorized or unlawful processing and against

its loss, destruction or accidental damage, through the application of technical measures

or appropriate organizational structures (“integrity and confidentiality”).”

In relation to this principle, Recital 39 of the aforementioned GDPR states that:

“[…]Personal data must be processed in a way that guarantees security and

appropriate confidentiality of personal data, including to prevent access

or unauthorized use of said data and of the equipment used in the treatment”.

The documentation in the file offers clear indications that the

claimed violated article 5.1 f) of the RGPD, principles related to treatment.

Although the claimed party states to this Agency that access to the data by

part of the claimant was in the exercise of her work activity and as a necessity

for the exercise of its tasks, the claimant proves having had access to

personal data that were not necessary for the exercise of said

activity, such as the complete history since the year 2017, of the emails

e-mail addresses of the employee she was replacing, with data on students from courses

past records, invoice data, withholding certificates from the previous employee,

phone, address.

In accordance with the evidence available at the present time of

agreement to initiate the sanctioning procedure, and without prejudice to what results from the

instruction, it is considered that the known facts could constitute a

infringement, attributable to the claimed party, for violation of article 5.1.f) of the

GDPR.

Classification of the infringement of article 5.1.f) of the RGPD

IV

If confirmed, the aforementioned infringement of article 5.1.f) of the RGPD could lead to the

commission of the offenses typified in article 83.5 of the RGPD that under the

The heading "General conditions for the imposition of administrative fines" provides:

“The infractions of the following dispositions will be sanctioned, in accordance with the

paragraph 2, with administrative fines of a maximum of EUR 20,000,000 or,

in the case of a company, an amount equivalent to a maximum of 4% of the

global total annual turnover of the previous financial year, opting for

the largest amount:

the basic principles for the treatment, including the conditions for the

a)

consent under articles 5, 6, 7 and 9; (…)”

In this regard, the LOPDGDD, in its article 71 "Infringements" establishes that

“The acts and behaviors referred to in sections 4,

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

contrary to this organic law.

For the purposes of the limitation period, article 72 “Infringements considered very

serious” of the LOPDGDD indicates:

"1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679,

considered very serious and will prescribe after three years the infractions that suppose

a substantial violation of the articles mentioned therein and, in particular, the

following:

a) The processing of personal data violating the principles and guarantees

established in article 5 of Regulation (EU) 2016/679. (…)”

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Article 32 of the GDPR

With regard to the application of data protection regulations to the alleged

raised, it must be taken into account that the RGPD, in its article 32, requires the

responsible for the treatment, the adoption of the corresponding measures of

security necessary to guarantee that the treatment is in accordance with the regulations

in force, as well as to guarantee that any person acting under the authority of the

responsible or of the person in charge and has access to personal data, can only treat them

following the instructions of the person in charge.

Article 32 of the RGPD, security of treatment, establishes the following:

"1. Taking into account the state of the art, the application costs, and the

nature, scope, context and purposes of the treatment, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical measures and

appropriate organizational measures to guarantee a level of security appropriate to the risk,

which in your case includes, among others:

a)

a)

b)

pseudonymization and encryption of personal data;

the ability to ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

the ability to restore availability and access to personal data

promptly in the event of a physical or technical incident;

c) a process of regular verification, evaluation and evaluation of the effectiveness

technical and organizational measures to guarantee the security of the

treatment.

2. When evaluating the adequacy of the security level, particular account shall be taken of

takes into account the risks presented by the processing of data, in particular as

consequence of the accidental or unlawful destruction, loss or alteration of data

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data.

3. Adherence to an approved code of conduct under article 40 or to a

certification mechanism approved under article 42 may serve as an element

to demonstrate compliance with the requirements established in section 1 of the

present article.

4. The person in charge and the person in charge of the treatment will take measures to guarantee that

any person acting under the authority of the person in charge or the person in charge and

has access to personal data can only process said data following

instructions of the person in charge, unless it is obliged to do so by virtue of the Right of

the Union or the Member States.

Recital 75 of the RGPD lists a series of factors or assumptions associated with

risks for the guarantees of the rights and freedoms of the interested parties:

“The risks to the rights and freedoms of natural persons, serious and
variable probability, may be due to the processing of data that could cause
physical, material or non-material damages, particularly in cases where
that the treatment may give rise to problems of discrimination, usurpation of
identity or fraud, financial loss, reputational damage, loss of
confidentiality of data subject to professional secrecy, unauthorized reversal of the
pseudonymization or any other significant economic or social damage; in the
cases in which the interested parties are deprived of their rights and freedoms or are
prevent exercising control over your personal data; In cases where the data
treated personalities reveal ethnic or racial origin, political opinions, religion
or philosophical beliefs, militancy in trade unions and the processing of genetic data,
data relating to health or data on sex life, or convictions and offenses
criminal or related security measures; In cases where they are evaluated
personal aspects, in particular the analysis or prediction of aspects related to the
performance at work, economic situation, health, preferences or interests
personal, reliability or behavior, situation or movements, in order to create or
use personal profiles; in the cases in which personal data of
vulnerable people, in particular children; or in cases where the treatment
involves a large amount of personal data and affects a large number of
interested.”

In the specific case under examination, by maintaining the same email account
electronically deregistering the previous tutor and registering the new one, would imply that the
security measures of the claimed entity are not adequate to the regulations of
data protection, assuming such facts the violation of article 32 of the RGPD.

Despite the fact that the claimant informed the respondent of the situation

by email, the same day they replied that the account they had

assigned, for economic and operational reasons, was the same used by the other

tutor being able to eliminate the folders that she considers opportune.

From the actions carried out, there is evidence of the existence of reasonable indications and

enough that the security measures, both of a technical nature and

organizations, with which the claimed party had in relation to the data that

undergoing treatment, were not adequate at the time of the gap in

security.

The consequence of this lack of security measures was the exposure to third parties of

Personal information. That is, those affected have been deprived of control

about your personal data.

This risk must be taken into account by the data controller, who must

establish the necessary technical and organizational measures to prevent the loss of

control of the data by the data controller and, therefore, by the data controllers.

holders of the data that provided them.

Without prejudice to what results from the investigation, at this time there is evidence

sufficient regarding the absence of adequate security measures. These

facts may constitute a violation of article 32 RGPD, without prejudice to

what results from the investigation of this file.

Classification of the infringement of article 32 of the RGPD

SAW

If confirmed, the aforementioned violation of article 32 of the RGPD could lead to the

commission of the offenses typified in article 83.4 of the RGPD that under the

The heading "General conditions for the imposition of administrative fines" provides:

“The infractions of the following dispositions will be sanctioned, in accordance with the

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

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

global total annual turnover of the previous financial year, opting for

the largest amount:

a)

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

11, 25 to 39, 42 and 43; (…)”

In this regard, the LOPDGDD, in its article 71 "Infringements" establishes that

“The acts and behaviors referred to in sections 4,

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

contrary to this organic law.

For the purposes of the limitation period, article 73 “Infringements considered serious”

of the LOPDGDD indicates:

“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

substantial violation of the articles mentioned therein and, in particular, the

following:

a) Failure to adopt those technical and organizational measures that

are appropriate to guarantee an adequate level of security when

risk of treatment, in the terms required by article 32.1 of the

Regulation (EU) 2016/679.”

7th

Sanction

In order to determine the administrative fine to be imposed, the

provisions of articles 83.1 and 83.2 of the RGPD, precepts that indicate:

"1. Each control authority will guarantee that the imposition of fines

administrative actions under this article for violations of this

Regulation indicated in sections 4, 5 and 6 are in each individual case

effective, proportionate and dissuasive.

2. Administrative fines will be imposed, depending on the circumstances of each

individual case, in addition to or as a substitute for the measures contemplated in the

Article 58, paragraph 2, letters a) to h) and j). When deciding to impose a fine

administration and its amount in each individual case will be duly taken into account:

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

nature, scope or purpose of the processing operation in question, as well as the number

number of interested parties affected and the level of damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor to pa-

allocate 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,

gives an account of the technical or organizational measures that have been applied by virtue of the

articles 25 and 32;

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

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

infringement and mitigate the possible adverse effects of the infringement;

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

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

whether the person in charge or the person in charge notified the infringement and, if so, to what extent.

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

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

the same matter, compliance with said measures;

j) adherence to codes of conduct under Article 40 or to certification mechanisms

approvals approved in accordance with article 42,

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

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

mind, through infraction."

For its part, article 76 "Sanctions and corrective measures" of the LOPDGDD

has:

"1. The penalties 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 section 2 of the aforementioned article.

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

may also be taken into account:

a) The continuing nature of the offence.

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

of personal data.

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 offence.

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

of the infringement, which cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

g) Have, when it is not mandatory, a delegate for the protection of

h) The submission by the person in charge or person in charge, with

voluntary, to alternative conflict resolution mechanisms, in those

data.

assumptions in which there are controversies between those and any

interested."

Sanction for the infringement of article 5.1.f) of the RGPD.

In accordance with the transcribed precepts, and without prejudice to what results from the

instruction of the procedure, in order to set the amount of the penalty for infringement

of article 5.1 f), it is appropriate to graduate the fine taking into account:

As an aggravating circumstance:

Article 83.2.a) RGPD: the nature, seriousness and duration of the infringement, taking

taking into account the nature, scope or purpose of the processing operation to be carried out.

concerned, as well as the number of interested parties affected and the level of damages

who have suffered:

The claimant informed the respondent of the situation. On 4/13/21 communicated

the facts by sending an email to the claimed entity. The same day he

They answered that the account they had been assigned is the one used by the other tutor,

being able to eliminate the folders that it considers opportune, therefore, the infraction
it was maintained the entire time the claimant was rendering her services.
Regarding the volume of treatments carried out, the claimant has access to the
Post history since 2017.
Article 76.2 b) LOPDGDD: "The link between the activity of the offender and the
tion of personal data processing". The activity of the claimed entity requires
continuous processing of personal data. Likewise, the entity claims
da carries out for the development of its activity, a high volume of damage treatment
personal cough.
Considering the exposed factors, the initial valuation that reaches the amount of the
fine is €3,000 for infringement of article 5.1 f) of the RGPD, regarding the
violation of the principle of confidentiality and €2,000 for violation of article 32
of the aforementioned RGPD, regarding the security of the processing of personal data.
viii
Responsibility
Establishes Law 40/2015, of October 1, on the Legal Regime of the Public Sector, in
Chapter III on the "Principles of the power to impose penalties", in article 28
under the heading "Responsibility", the following:
"1. They may only be sanctioned for acts constituting an administrative infraction.
natural and legal persons, as well as, when a Law recognizes their capacity to
to act, the affected groups, the unions and entities without legal personality and the
independent or autonomous estates, which are responsible for them
title of fraud or guilt."

Lack of diligence in implementing appropriate security measures

with the consequence of breaching the principle of confidentiality constitutes the

element of guilt.

IX

Measures

If the infraction is confirmed, it could be agreed to impose on the person responsible the adoption of

appropriate measures to adjust their actions to the regulations mentioned in this

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

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

treatment that the treatment operations comply with the provisions of the

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

specified period…”. The imposition of this measure is compatible with the sanction

consisting of an administrative fine, as provided in art. 83.2 of the GDPR.

It is warned that not meeting the requirements of this organization may be

considered as an administrative offense in accordance with the provisions of the RGPD,

typified as an infraction in its article 83.5 and 83.6, being able to motivate such conduct the

opening of a subsequent sanctioning administrative proceeding.

Therefore, in accordance with the foregoing, by the Director of the Agency

Spanish Data Protection,

HE REMEMBERS:

FIRST: START A SANCTIONING PROCEDURE FOR EUROPEAN STUDIES

DE POSTGRADO Y EMPRESA, S.L., with NIF B86256419, for the alleged infringement

of article 5.1. f) of the RGPD, typified in accordance with the provisions of article 83.5 of the

RGPD, qualified as very serious for prescription purposes in article 72.1 a) of the

LOPDGDD.

SECOND: INITIATE PUNISHMENT PROCEDURE for EUROPEAN STUDIES

DE POSTGRADO Y EMPRESA, S.L., with NIF B86256419, for the alleged infringement

of article 32 of the RGPD, typified in accordance with the provisions of article 83.4 of the

cited RGPD, qualified as serious for prescription purposes in article 73

section f) of the LOPDGDD.

THIRD: APPOINT instructor to B.B.B. and, as secretary, to C.C.C., indicating

that any of them may be challenged, where appropriate, in accordance with the provisions of

Articles 23 and 24 of Law 40/2015, of October 1, on the Legal Regime of the

Public Sector (LRJSP).

FOURTH: INCORPORATE to 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 Subdirectorate General for Inspection of

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

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

October, of the Common Administrative Procedure of the Public Administrations, the

The corresponding sanction would be €3,000 for infraction of article 5.1 f) of the

RGPD, regarding the violation of the principle of confidentiality and €2,000 per

infringement of article 32 of the aforementioned RGPD, regarding the security of the treatment of

personal data, without prejudice to what results from the instruction.

SIXTH: NOTIFY this agreement to ESTUDIOS EUROPEOS DE

POSTGRADO Y EMPRESA, S.L., with NIF B86256419, granting it a term of

hearing of ten business days to formulate the allegations and present the

tests you deem appropriate. In your statement of arguments, you must provide your

NIF and the procedure number that appears in the heading of this

document.

If within the stipulated period it 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, of 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 term granted for the formulation of allegations to the

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

sanction to be imposed in this proceeding. With the application of this

reduction, the sanction would be established at FOUR THOUSAND EUROS, resolving the

procedure with the imposition of this sanction.

Similarly, you 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 in FOUR THOUSAND EUROS, and its payment will imply the

termination of the procedure.

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

apply for the acknowledgment of responsibility, provided that this acknowledgment

of the responsibility is revealed within the period granted to formulate

arguments at the opening of the procedure. The 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 it were appropriate to apply both reductions, the amount of the penalty would be

set at THREE THOUSAND EUROS.

In any case, the effectiveness of any of the two reductions mentioned will be conditioned to the abandonment or renunciation of any action or resource in via administrative against the sanction.

In case you chose to proceed to the voluntary payment of any of the amounts indicated above, you must make it effective by depositing it in account no. ES00 0000 0000 0000 0000 0000, opened on behalf of the Spanish Agency for Data Protection, in the banking entity CAIXABANK, S.A., indicating in the concept the reference number of the procedure that appears in the heading of this document and the reason for the reduction of the amount to which it avails itself.

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

The procedure will have a maximum duration of nine months from the date of the start-up agreement or, where appropriate, of the draft start-up agreement. Once this period has elapsed, it will expire 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, in what successively, the notifications sent to you will be made exclusively in a electronically by appearance at the electronic headquarters of the General Access Point of the Administration or through the unique Authorized Electronic Address and that, if not

access them, their rejection will be recorded in the file, considering the

processing and following the procedure. You are informed that you can identify before this

Agency an email address to receive the notice of commissioning

disposition of the notifications and that the lack of practice of this notice will not prevent

that the notification be considered fully valid.

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

LPACAP, there is no administrative appeal against this act.

Sea Spain Marti

Director of the Spanish Data Protection Agency

>>

935-110422

SECOND: On June 2, 2022, the claimed party has proceeded to pay

the sanction in the amount of 3000 euros making use of the two planned reductions

in the Startup Agreement transcribed above, which implies the recognition of the

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 resource in via

administrative action against the sanction and acknowledgment of responsibility in relation to

the facts referred to in the Initiation Agreement.

FOURTH: In the Initial Agreement transcribed above, it was stated that,

If the infringement is confirmed, it could be agreed to impose on the person responsible the adoption of

appropriate measures to adjust their actions to the regulations mentioned in this

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

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

treatment that the treatment operations comply with the provisions of the

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

specified period…”.

Having recognized the responsibility for the infraction, the imposition of

the measures included in the Initiation Agreement.

FOUNDATIONS OF LAW

Yo

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

(General Data Protection Regulation, hereinafter RGPD), 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 Agency for Data Protection will be governed by the provisions

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

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures."

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:

"1. 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."

According to what was stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: TO DECLARE the termination of procedure EXP202102806,

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

SECOND: REQUIRE EUROPEAN POSTGRADUATE AND BUSINESS STUDIES,

SL so that within a period of one month it notifies the Agency of the adoption of the measures

that are described in the legal grounds of the Initiation Agreement transcribed in the

this resolution.

THIRD: NOTIFY this resolution to ESTUDIOS EUROPEOS DE

POSTGRADUATE AND COMPANY, 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 Spanish Data Protection Agency