 File No.: PS/00135/2022

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 June 13, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against UNONO NET 3.0,

SL (hereinafter, the claimed party), through the Agreement that is transcribed:

<<

File No.: PS/00135/2022

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: D.A.A.A. (hereinafter, the complaining party), on May 24,

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

claim is directed against UNONO NET 3.0, S.L., with NIF B86302510 (hereinafter,

the claimed party). The grounds on which the claim is based are as follows:

A security breach has occurred by the data controller, such as

consequence of sending an email to multiple recipients without

use the blind copy functionality.

The message is sent by a human resources agency and the recipients are

dozens of candidates who, supposedly, have provided their CV so that they can

report job offers compatible with your profile.

Along with the claim, it provides an email sent on May 20,

2021, in which the email addresses of the rest of the

recipients to whom the shipment was also addressed.

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

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

hereinafter LOPDGDD), said claim was transferred to the claimed party, to

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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 regulations of

Data Protection.

The transfer, which was carried out by electronic notification, in accordance with the regulations

established in Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations (hereinafter, LPACAP), was received on the date

July 5, 2021, as stated in the certificate in the file.

No response has been received to this transfer letter.

THIRD: On September 8, 2021, in accordance with article 65 of the

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

FOURTH: The General Subdirectorate for Data Inspection proceeded to carry out

of previous investigative actions to clarify the facts in

question, by virtue of the functions assigned to the control authorities in the

article 57.1 and the powers granted in article 58.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter RGPD), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the

LOPDGDD, having knowledge of the following extremes:

Date of notification to the AEPD of a data security breach

personal: May 24, 2021, on the part of a claim.

Breach detection date: 05/20/2021.

Number of affected according to notification: (...).

Type of data according to notification: (...).

INVESTIGATED ENTITY

UNONO NET 3.0, S.L. with NIF B86302510, and address at AVDA CARDENAL

HERRERA ORIA 173, 12º C - 28034 MADRID (MADRID)

The notifying entity is a limited company of Spanish nationality.

According to the data in AXESOR, it is an SME with 7 employees and a

sales volume of 3758 euros.

On January 25, 2022, a reiteration of the request for information was sent

reclaimed. Upon such request, the respondent requests information on the claim

original.

On 02/10/2022, the original claim is transferred to you requesting information on

the gap. No response has been given to this request.

On 02/17/2022, an attempt was made to contact the company by telephone, using

number ***TELEPHONE.1 that appears on the AXESOR page, being impossible

contact them. It proceeds to call another number found on the internet

(***PHONE.2). It was also not possible to contact.

Finally, an email is sent to the DPD, to an address found in the

website of the person claimed (privacy@unono.net), which was rejected.

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

carrying out personal data processing, since UNONO NET 3.0,

S.L., is an emerging recruitment and selection company, with thousands of users and

associated companies on its platform that, for the development of their activity of

staffing and selection of personnel, 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 purposes and means of treatment; if the law of the Union or of the Member States determines determines the purposes and means of the treatment, the person responsible for the treatment or the criteria specific for their appointment may be established by the Law of the Union or of the Member states.

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 an email has been sent from the email address: ***EMAIL.1 email to (...) recipients approximately, (...).

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.

Within the principles of treatment provided for in article 5 of the RGPD, the

integrity and confidentiality of personal data is guaranteed in section 1.f)

of article 5 of the RGPD. For its part, the security of personal data comes

regulated in articles 32, 33 and 34 of the RGPD, which regulate the security of the

treatment, notification of a violation of the security of personal data to

the control authority, as well as the communication to the interested party, respectively.

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.

In the present case, according to the documentation provided by the claimant and in the absence of

response from the respondent, it can be verified that, from the address of

email: ***EMAIL.1 an email has been sent to (…) recipients

about, (…).

Sending an email to a plurality of recipients without hiding them from

each of them the email addresses of the rest of the recipients to whom

that the shipment was also addressed, could constitute, on the part of the claimed, in its

condition of responsible for the aforementioned processing of personal data, a

violation of the principle of confidentiality, by disseminating that information among the

recipients of the shipment without stating that he had obtained the consent of the

same for that specific treatment.

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. (…)”

v

Article 32 of the GDPR

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) pseudonymization and encryption of personal data;

b) the ability to ensure the confidentiality, integrity, availability and
permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data
quickly in the event of a physical or technical incident;

d) 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.

From the documentation in the file, there are clear indications that the

claimed has violated article 32 of the RGPD, when a security incident occurred.

when sending an email to a large number of recipients, without the

blind copying, without having the appropriate technical and organizational measures.

It should be noted that the RGPD in the aforementioned precept does not establish a list of the

security measures that are applicable according to the data that are subject

of treatment, but establishes that the person in charge and the person in charge of the treatment

apply technical and organizational measures that are appropriate to the risk involved

the treatment, taking into account the state of the art, the application costs, the

nature, scope, context and purposes of the treatment, the risks of probability

and seriousness for the rights and freedoms of the persons concerned.

Likewise, the security measures must be adequate and proportionate to the

detected risk, pointing out that the determination of technical measures and

organizational must be carried out taking into account: pseudonymization and encryption,

capacity to guarantee confidentiality, integrity, availability and resilience, the

ability to restore availability and access to data after an incident, process

verification (not audit), evaluation and assessment of the effectiveness of the

measures.

In any case, when evaluating the adequacy of the level of security,

particularly taking into account the risks presented by the processing of data, such 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 and that could cause damages physical, material or immaterial.

In this same sense, recital 83 of the RGPD states that:

"(83) In order to maintain security and prevent the treatment from violating the provided in this Regulation, the person in charge or the person in charge must evaluate the risks inherent to the treatment and apply measures to mitigate them, such as encryption. These measures must guarantee an adequate level of security, including confidentiality, taking into account the state of the art and the cost of its application regarding the risks and the nature of the personal data that must be protect yourself. When assessing the risk in relation to data security, take into account the risks arising from the processing of personal data, such as the accidental or unlawful destruction, loss or alteration of personal data transmitted, stored or otherwise processed, or the communication or access is not authorized to said data, susceptible in particular to cause damages physical, material or immaterial.

The responsibility of the claimed party is determined by the lack of preventive measures. security, since it is responsible for making decisions aimed at implementing effectively the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk to ensure the confidentiality of the data, restoring their availability and preventing access to them in the event of an incident physical or technical. However, the documentation provided shows that the entity has not only failed to comply with this obligation, but also the adoption of measures in this regard, despite having notified him of the claim presented.

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 32 of the RGPD.

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:

f) The lack of adoption of 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

assumptions in which there are controversies between those and any

interested."

data.

Considering the exposed factors, the initial valuation that reaches the amount of the

fine is €1,000 for infringement of article 5.1 f) of the RGPD, regarding the

violation of the principle of confidentiality and €500 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 SANCTION PROCEDURE against UNONO NET 3.0, S.L., with

NIF B86302510, 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, classified as very serious to

effects of prescription in article 72.1 a) of the LOPDGDD.

SECOND: START SANCTION PROCEDURE against UNONO NET 3.0, S.L.,

with NIF B86302510, for the alleged infringement of article 32 of the RGPD, typified

in accordance with the provisions of article 83.4 of the aforementioned RGPD, classified as serious to

effects of prescription 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 €1,000 for infraction of article 5.1 f) of the
RGPD, regarding the violation of the principle of confidentiality and €500 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 UNONO NET 3.0, S.L., with NIF
B86302510, granting him a hearing period of ten business days to formulate
the allegations and present the evidence it deems appropriate. In his writing of
allegations you must provide your NIF and the procedure number that appears in the
header 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 penalty would be established at ONE THOUSAND TWO HUNDRED EUROS (€1,200)
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 at ONE THOUSAND TWO HUNDRED EUROS (€1,200) 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 NINE HUNDRED EUROS (€900).

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 July 1, 2022, the claimed party has proceeded to pay

the sanction in the amount of 900 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.

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 and 48.1 of the Law

Organic 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 Data Protection Agency.

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 PS/00135/2022, of

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

SECOND: NOTIFY this resolution to UNONO NET 3.0, 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