 File No.: EXP202205819

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 14, 2023, the Director of the Spanish Agency for

Data Protection agreed to start a sanctioning procedure against GRUPO DE

GLOBAL SECURITY AND CONTROL, S.L. (hereinafter, the claimed party),

through the Agreement that is transcribed:

<<

File No.: EXP202205819

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: D.A.A.A. (hereinafter, the claiming party), on May 18,

2022, filed a claim with the Spanish Data Protection Agency. The

The claim is directed against GRUPO DE SEGURIDAD Y CONTROL GLOBAL, S.L.

with NIF B87977005 (hereinafter, the claimed party). The reasons on which the

claim are as follows:

The complaining party states that he works in the security company called

GLOBAL SECURITY AND CONTROL GROUP, S.L.

The members of said company have formed a group in the application of

WhatsApp, among which is the claimant.

Indicates that you performed a specific service in the security checkpoint of the company, place

where the video surveillance cameras are located and that his boss requested that they be

uploaded to said WhatsApp group, the video at the moment in which, a

alarm from a home security camera.

The video was uploaded by another worker.

In this video appears the image of the claimant during his working day.

He considers that his consent for such dissemination has not been requested and that the video was

disseminated with the purpose of harassing him before the rest of the workers who are members of the

Work WhatsApp group.

Provide an image of the WhatsApp group where the recording was published, a copy of the

broadcast recording and complaint filed with the Civil Guard for the facts

Of claim.

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 established 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), by means of electronic notification, was received in

dated May 27, 2022, as stated in the certificate in the file.

On June 24, 2022, this Agency received a written response

indicating:

-That the person responsible for the treatment and owner of the video surveillance cameras is the

Community of Owners of A.A.A..

-That the person responsible for the Treatment and Grupo de Seguridad y Control Global, S.L.,

as the person in charge of the treatment, have formalized a contract for the provision of

surveillance and protection services between the parties and a contract for the person in charge of

processing of personal data.

-That the claim and request for information on video surveillance systems

should be addressed to the person responsible for the treatment: Community of Owners of A.A.A..

-That on May 15, 2022, at approximately 11:20 p.m., the chief

of Security of (...), received a call from the control center of the service of

surveillance warning of the intrusion of several individuals inside one of the houses,

of the urbanization of A.A.A..

The guard who was in the control center at that moment detected in the

cameras, as four hooded men fled the urbanization and proceeded to give

instructions to both the (...) patrol and the Civil Guard, where there was a

attempted pursuit with no luck in arrest.

- That the head of Security initiated an investigation into the facts within his

functions, reviewing cameras and coordinating the action with the Civil Guard and the

Security Guards who were part of the service facilitating the Guard itself

Civil, all the information requested.

In said investigation, the control center was asked to provide the images of the events to coordinate the team and make the appropriate decisions through of the internal messaging application in which team members are coordinated.

Through said WhatsApp Group, the images related to the intrusion to inform the Civil Guard of the current situation and comply with their professional obligations of collaboration with the Security Forces and Corps of the State in an emergency situation and risk to people and property.

-That the workers of Grupo de Seguridad y Control Global who provide services in that urbanization communicate through the aforementioned messaging application to share files and information relevant to the service and through a circuit private band closed by professional walkies. They are all aware of their obligations and sign a confidentiality agreement, so they know that the images and personal data subject to processing must be treated in a manner totally confidential and with the sole purpose of fulfilling the order professional.

-Indicates that unusual behavior of the security guard is observed in the videos and complainant before the AEPD, for which the head of Security informs and complaint to the Territorial Delegation of the National Police, specifically the Department of Private Security, the events that occurred to investigate whether there could be a collaboration or link between the security guard and the intrusion happened.

The worker and claimant was later dismissed with disciplinary action. Police Nacional accepts the complaint for processing and proceedings are opened in this regard that

They are currently the subject of judicial investigation.

- He believes that the reasons for this claim are an attempt at retaliation by the claimant as a result of disciplinary dismissal, by negligently failing to comply with his obligations, absent from his job on the day and time of the events and being reported to the authorities.

- Based on the foregoing, it states that the request for recordings through the messaging application in order to urgently provide them to the Guard Civil is adequate, pertinent, proportional, not excessive and suitable to guarantee the intended purposes.

THIRD: On August 18, 2022, in accordance with article 65 of the LOPDGDD, the admission for processing of the claim presented by the complaining party.

FOURTH: according to the report collected from the AXESOR tool, the entity GRUPO DE SEGURIDAD Y CONTROL GLOBAL, S.L is a small company, Established in 2017, with an estimated turnover of ***QUANTITY. € in the year 2021.

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 Agency for

Data Protection.

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

breached obligation

In the present case, we proceed to examine the claim presented, through

which transfers the alleged non-consensual access to the images obtained by the

recording system of the Community of Owners, being the object, according to

manifestation of the complaining party, of its dissemination in a WhatsApp group.

It is, therefore, pertinent to analyze whether the processing of personal data carried out through

through its dissemination in a WhatsApp group is in accordance with the provisions of the

GDPR.

The physical image of a person, according to article 4.1 of the GDPR, is data

personnel and their protection, therefore, is the object of said Regulation, understanding by

personal data: "all information about an identified natural person or

identifiable".

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

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

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

one or several elements proper to physical, physiological, genetic, psychological,

economic, cultural or social of said person.

The GDPR defines "processor" or "in charge" as the natural person or

legal entity, public authority, service or other body that processes personal data for

account of the data controller; And "responsible for the treatment" or "responsible for

ble' is the natural or legal person, public authority, service or other body which,

alone or together with others, determine the purposes and means of the processing.

In the present case, the Community of owners holds the status of "responsibility

of the treatment" (article 4 point 7 of the GDPR), entrusting the insurance company

As the person in charge of the treatment, the provision of the security service: security

ence and protection of the Urbanization of A.A.A..

For the correct provision of said service, the person in charge of the treatment must access

give personal data.

In compliance with the provision to which it is committed by means of the contract of

service lease, the claimed party shall have all its own obligations

established, respecting in any case the current regulations on protection

of personal data, as well as the remaining regulations of the legal system

co in force Among them, the fact that personal data is treated in such a way

that adequate security of the same is guaranteed, including protection against

unauthorized or illegal treatment and against its loss, destruction or accidental damage,

through the application of appropriate technical or organizational measures.

II

Article 5.1.f) of the GDPR

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

"Article 5 Principles relating to treatment:

1. Personal data will be:

(…)

f) processed in such a way as to guarantee adequate data security

personal data, including protection against unauthorized or unlawful processing and against

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

or organizational procedures (“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”.

Video surveillance in a community consists of installing cameras in the

common elements of the building that allows to improve surveillance and therefore the

security within it. At the time of its installation, it is necessary to comply with the

obligations contained in the European Data Protection Regulation and the Law

Organic 3/2018, Protection of Personal Data and Guarantee of Rights

digital.

Access to the recordings of video surveillance systems can only occur

in the cases determined by law and by a person duly authorized in

his case, being equally “exceptional” the dissemination of the images that have been

obtained with them, respecting in any case the current regulations on

protection of personal data, as well as the other regulations of the

legal system in force.

In the video attached to the claim, which lasts 21 seconds, you can

observe the existence of a camera installed in the upper part, being able to

Visualize the image of the interior of the checkpoint with a worker inside.

The documentation in the file offers clear indications that the party

claimed violated article 5.1 of the GDPR, principles relating to treatment, all

time you proceeded to send personal data (images) of the party

claimant to a group of people, violating the principle of confidentiality,

established in the aforementioned article 5.1.f) of the GDPR.

In accordance with the evidence available at the present time of

agreement to start the disciplinary procedure, and without prejudice to what results from the

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

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

GDPR.

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

IV.

If confirmed, the aforementioned violation of article 5.1.f) of the GDPR could lead to the

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

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

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

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

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

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

the highest amount:

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

to)

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

In this regard, the LOPDGDD, in its article 71 "Infractions" 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 "Infractions considered very

serious” of the LOPDGDD indicates:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679,

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

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

following:

a) The processing of personal data in violation of the principles and guarantees

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

V

GDPR Article 32

Article 32 of the GDPR, 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 processing, 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 and
appropriate organizational measures to guarantee a level of security appropriate to the risk,
which may include, among others:

a) the 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 assessment of effectiveness
technical and organizational measures to guarantee the safety of the
treatment.

2. When evaluating the adequacy of the security level, particular consideration will be given to
take into account the risks presented by data processing, in particular as
consequence of the destruction, loss or accidental or illegal alteration of data
personal information transmitted, preserved or processed in another way, or the communication or
unauthorized access to such data.

3. Adherence to an approved code of conduct pursuant to 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 controller and the processor shall take measures to ensure that
any person acting under the authority of the controller or processor and
have access to personal data can only process such data by following
instructions of the person in charge, unless it is obliged to do so by virtue of the Law of

the Union or of the Member States.

The facts revealed imply the lack of technical and organizational measures

you are going to send personal data (images) of the complaining party to a group

of people without adequate guarantees through a well-known messaging application-

would with the consequent lack of diligence, allowing access to said data.

As stated in the response brief dated June 24, 2022, the

workers of Grupo de Seguridad y Control Global who provide services in the

urbanization, communicate through a WhatsApp group to share

files and information relevant to the service, through a closed circuit of

private band by professional walkies. However, the use of the aforementioned

messaging application is common for communication and sending documents and

images, it must be taken into account to whom the messages are sent when in the

they include personal data, since there must be a justification for

send personal data to members of a WhatsApp group. In this case

In particular, the use of the medium is not assessed, that is, the application of

instant messaging, but the sending of certain information with data

personal to a group of people.

And if, in addition, the purpose was to inform the Civil Guard of the situation and comply

with their professional obligation to collaborate with the Security Forces and Corps

of the State, it was not necessary to send the images through a group, but

simply pass them on to the head of security and he to the Forces and Bodies of

State Security.

The responsibility of the defendant is determined by the lack of measures of

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, reducing the number of workers with access to information

personnel, so that there is no unnecessary or excessive access by

of the workers, as well as avoiding the reproduction or unjustified forwarding of

Personal information.

In accordance with the evidence available at the present time of

agreement to start disciplinary proceedings, and without prejudice to what results from the

instruction, it is considered that there is sufficient evidence regarding the absence of

adequate security measures.

The known facts could constitute an infringement, attributable to the party

claimed, for violation of article 32 GDPR.

Classification of the infringement of article 32 of the GDPR

SAW

If confirmed, the aforementioned infringement of article 32 of the GDPR could lead to the

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

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

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 highest amount:

to)

the obligations of the controller and the person in charge under articles 8,

11, 25 to 39, 42 and 43; (…)”

In this regard, the LOPDGDD, in its article 71 "Infractions" 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 "Infractions considered serious"

of the LOPDGDD indicates:

"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:

f) The lack of adoption of those technical and organizational measures that

are appropriate to ensure a level of security appropriate to the

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

Regulation (EU) 2016/679.”

VII

Sanction proposal

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

provisions of articles 83.1 and 83.2 of the GDPR, precepts that state:

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

administrative proceedings under this article for violations of this

Regulations 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 in lieu of the measures contemplated in

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

administration and its amount in each individual case shall 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 person in charge or in charge of the treatment to

settle 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, habi-

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 controller or processor;

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

determine whether the controller or processor notified the infringement and, if so, to what extent

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

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

the same matter, compliance with said measures;

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

fications approved in accordance with article 42,

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

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

mind, through infraction."

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

has:

"1. The sanctions provided for in sections 4, 5 and 6 of article 83 of the Regulation

(UE) 2016/679 will be applied taking into account the graduation criteria

established in section 2 of said 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) Linking the activity of the offender with the performance of processing

of personal data.

c) The benefits obtained as a consequence of the commission of the infraction.

d) The possibility that the conduct of the affected party could have led to the

commission of the offence.

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

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

f) The affectation of the rights of minors.

g) Have, when it is not mandatory, a data protection delegate

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

voluntary, alternative conflict resolution mechanisms, in those

cases in which there are controversies between those and any

interested."

data.

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

fine is €2,000 for violation of article 5.1 f) of the GDPR, regarding the

violation of the principle of confidentiality and €1,000 for violation of article 32

of the aforementioned GDPR, regarding the security of the processing of personal data.

VIII

adoption of measures

If the infringement is confirmed, it could be agreed to impose on the person responsible 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…". The imposition of this measure is compatible with the sanction

consisting of an administrative fine, 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, in accordance with the foregoing, by the Director of the Agency

Spanish Data Protection,

HE REMEMBERS:

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

11/14

FIRST: INITIATE SANCTION PROCEDURE for SECURITY GROUP

Y CONTROL GLOBAL, S.L., with NIF B87977005,

- For the alleged infringement of article 5.1.f) of the GDPR, classified in accordance with the

provided in article 83.5 of the GDPR, classified as very serious for the purposes of

prescription in article 72.1 a) of the LOPDGDD.

- for the alleged infringement of article 32 of the GDPR, classified in accordance with the provisions

in article 83.4 of the GDPR, classified as serious for the purposes of prescription in the

Article 73 f) of the LOPDGDD.

SECOND: 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).

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

claim filed by the claimant and its documentation, the

documentation provided by the claimed party, as well as the documents obtained and

generated by the General Sub-directorate of Data Inspection in the proceedings

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, the

sanction that could correspond would be, for the alleged violation of article 5.1.f)
of the GDPR, typified in article 83.5 of said regulation, an administrative fine of
amount 2,000.00 euros and for the alleged infringement of article 32 of the GDPR, typified
in article 83.4 of said regulation, administrative fine amounting to 1,000.00 euros

FIFTH: NOTIFY this agreement to SECURITY AND CONTROL GROUP
GLOBAL, S.L., with NIF B87977005, granting it a hearing period of ten days
able to formulate the allegations and present the evidence that it considers
convenient. In your statement of allegations you must provide your NIF and the number of
procedure that appears in the heading 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 2,400.00 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 2,400.00 euros and its 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 1,800.00 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.

In the event that you choose to proceed with the voluntary payment of any of the amounts indicated above (2,400.00 euros or 1,800.00 euros), you must make it effective by entering the account number IBAN: ES00-0000-0000-0000-0000-0000 (BIC/SWIFT Code: CAIXESBBXXX) opened in the name of the Spanish Agency for Protection of Data 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 accepts.

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.

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 24, 2023, the claimed party has proceeded to pay

of the sanction in the amount of 1800 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.

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 EXP202205819, in

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

SECOND: NOTIFY this resolution to SECURITY GROUP AND

CONTROL GLOBAL, 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

936-040822

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es