 Procedure No.: PS/00360/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claimant) on 06/08/2020 filed

claim before the Spanish Data Protection Agency. The claim is

directed against UST GLOBAL ESPAÑA, S.A., with NIF A84816644 (hereinafter, UST

GLOBAL or the one claimed). The reasons on which the claim is based are, in summary:

the claimant works for the consulting firm UST GLOBAL, which is providing services to

OpenBank; On 01/08/2020, the respondent notified OpenBank, by email

email, that two new employees would join the project (one of them the

claimant), for those who requested access to the VPN and other

Applications; in said email, sent with a copy to both employees,

provided their first and last names, professional emails, and phone numbers.

DNI. The complainant points out in this regard that such communication should have been made

independently, so that he would not have knowledge of the data of his

partner and vice versa.

Provide a copy of the email that motivates the complaint, dated 01/08/2020,

whose details are outlined in the Fourth Proven Fact.

SECOND: On 06/16/2020, the claim was transferred to UST GLOBAL so that

proceed to its analysis.

On 07/15/2020, in response to said transfer, the entity claimed reported that the

claimant was employed in that entity from 02/25/2019 until the day

04/03/2020.

As for the facts denounced, he pointed out that his actions were within

of the parameters of reasonableness and respect for privacy and the protection of

data under a criterion of balance between business efficiency and the implementation of

rigorous controls; that they were two employees who were going to join the

management of a project in Grupo Santander jointly and that sending the data of

both to the person in charge, to grant them access privileges within the framework of the

commission, did not seem to constitute an action that exceeded the limits that the

rules impose; that for this treatment the consent of the

employee; and that article 5.1.f) of the RGPD or 5 of the

LOPDGDD. It considers that UST GLOBAL limited itself to fulfilling an obligation

contract contracted with a client.

That no measure has been adopted by the respondent, considering that the action

referred to in the filed complaint is adjusted to the rules on protection of

data. That the complaint has been brought to the attention of the person responsible for

HR and the facts will be assessed, together with the DPD, taking into account

take into account the possible opinion of the Spanish Agency for Data Protection, in case in the

future it was considered necessary to avoid that, even in the case of two people who

are going to collaborate on a project with a client, their data must be sent separately

to the recipient, or otherwise encrypt or protect by security measures.

adequate security.

THIRD: On 10/07/2020, in accordance with article 65 of the LOPDGDD, the

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

claim filed.

FOURTH: On 11/05/2020, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the claimed party, in accordance with

the provisions of articles 63 and 64 of Law 39/2015, of October 1, of the

Common Administrative Procedure of Public Administrations (hereinafter,

LPACAP), for the alleged infringement of article 5.1.f) of the RGPD, typified in the

article 83.5.a) of the same legal text, determining that the sanction that could

correspond would amount to a total of 5,000 euros (five thousand euros), notwithstanding the

resulting from the instruction.

FIFTH: Having been notified of the aforementioned initiation agreement, the respondent submitted a written

allegations on 11/24/2020, in which he requests that the non-existence of

infraction and proceed to file the proceedings. Subsidiarily requests that

agree the warning with the imposition of corrective measures. In short, the

The aforementioned entity bases its request on the following considerations:

. Invokes the annulment of the initiation agreement, considering that in its Grounds

of Law refers to a possible infringement of article 5.1.f) of the RGPD and in its

operative part agrees to open sanctioning proceedings for an alleged

infringement of article 6 of the same Regulation, which has not been infringed, for

how much the sending made of the data of the employees in the framework of a contract of

services is protected by this article 6, in section 1.f) (legitimate interest).

The defendant considers that the first article cited has not been violated either.

. Declares reproduced the allegations made on the occasion of the transfer process,

which are outlined in the Second Antecedent. Understand that sending the mail

object of the claim, providing the person responsible for bank security

client the data (name and surnames, DNI and email) of the people who

are going to provide services in said entity, does not constitute a treatment that does not guarantee adequate security of the data, nor due to a hypothetical illicit treatment, nor for its potential loss, destruction or accidental damage. It was limited to completing a contractual obligation, identifying employees to the customer, in compliance of contractual agreements on information security.

It also points out that both the defendant and her client maintain technical measures and adequate organizational (provides ISO certification on the security system of the information that the respondent maintains in Spain).

You understand that this is not a personal data breach or that, if considered

Thus, due to access to the claimant's data by a colleague, it does not produce a damage to privacy, taking into account the type of data processed on the occasion of sending corporate.

. In any case, the defendant maintains a proactive responsibility, having appointed a DPO, despite not being required to do so; has outsourced this function for the DPO to maintain greater independence from the company; has sufficient internal resources in the Quality Area, with responsibility for the compliance with data protection regulations by the entity; It includes security information on the corporate intranet, available to employees; the external DPO has certified the completion of the adaptation processes to the RGPD and to the LOPDGDD; has a "Welcome Manual" for new employees, which includes privacy information; maintains privacy and security policies

the right information.

Provides various documentation on the points indicated, so that it is taken into account.

account when drafting the motion for a resolution:

. Use and security policy.

. Employee training.

. Data protection policy.

. Privacy policy addressed to suppliers and subcontractors.

. Awareness plans aimed at employees (2019 and 2020).

. In relation to the graduation of the sanction, it considers that the factors

following:

. There is no intention or negligence in sending information to a

Santander Group company, which is obliged to apply control measures

in data processing.

. The interested party has not suffered any damage or harm, both for the data

affected as by the framework in which they were shared.

. It is about two employees who work together and knew each other.

. Sending data to third parties is done through file sharing

electronic, so that none of those affected can see the data

others' personal.

. The defendant has not committed any infraction in this matter.

. Personal data does not belong to special categories.

. The claimed party has no special connection with data processing, nor

this constitutes its main activity. It is solely responsible for the data

of its employees, candidates, freelancers who provide service and

contact details of employees of corporate clients.

. The infraction is not continuous.

. He has not obtained any benefit from the facts claimed.

. You have DPD without being obliged to do so.

. After knowing the complaint, it was transferred to HR and DPD so that they

assess a new communication plan; and communicated to those responsible for

area and supervisors reminding them of the need to monitor safety controls

security.

SIXTH: On 11/30/2020, the instructor of the procedure agreed to open

a period of practical tests, agreeing on the following:

- Consider reproduced for evidentiary purposes the claim filed by the

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

Inspection Services that are part of file E/05043/2020.

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

PS/00360/2020 presented by the respondent and the documentation that they

accompanies.

SEVENTH: On 03/16/2021, the respondent entity filed a new writ of

allegations stating that it has continued to develop its compliance program

regarding the protection of privacy and personal data, having given

again specific training for all employees with evaluation tests,

which includes aspects related to the sending of information through the

email.

It is accompanied by a document related to this basic level training, which includes a

“Guide to good practices for sending confidential information and/or data

personal information to clients and/or suppliers”, in which it is pointed out that the sending of e-mails

with personal data of employees must be done individually, which

will prevent events similar to those reported in the future from occurring.

EIGHTH

: Dated 05/25/2021, by the General Subdirectorate for Data Inspection

access to the information available on the entity UST GLOBAL in "Axesor". In

said website has a turnover in the 2018 financial year, the last financial year

presented, of 46,395,898 euros and a result for the year of -2,008,626 euros.

Likewise, it is indicated that it is a medium-sized company, with 689 employees.

According to the information that appears in the Central Mercantile Registry, the "Subscribed Capital"

amounts to 60,104 euros

NINTH: On 05/27/2021, a resolution proposal was formulated, in the sense of

that the Director of the Spanish Data Protection Agency sanction the

entity UST GLOBAL, for an infringement of article 5.1.f) of the RGPD, in relation to

article 5 of the LOPDGDD, typified in article 83.5.a) of the RGPD, and qualified

as very serious for prescription purposes in article 72 of the LOPDGDD, with a

fine amounting to 5,000 euros (five thousand euros).

Notified of the aforementioned proposed resolution, dated 06/09/2021, it was received in this

Written agency of the UST GLOBAL entity in which it formulates the allegations

following:

. Reiterates, as a cause of defenselessness, that the initial agreement did not clearly specify the infringement allegedly committed, which led him to elaborate his answer around to the legality of the transfer of data made to OpenBank based on legitimate interest concurrent. Only by diligence it was considered convenient to make reference to the sending of the email in question to the two co-workers.

. The inclusion of the DNI of the two employees in that email does not imply, in the work environment in which the events occurred, a disclosure of data confidential information constituting an infringement. He adds that it is likely that both colleagues had knowledge of the other's DNI, due to the development of their own worked.

The same proposed resolution considers that “the interested party has not suffered damage or any damage, both for the data affected and for the framework in which it is shared” and that “these are two employees who work together and knew each other among them".

. Regarding the graduation of the fine, in a subsidiary way it indicates that the sanction proposed by the disclosure of the ID number of a worker to others is excessive, even more so considering that the proposal maintains the same sanction determined in the opening of the procedure, despite correcting the aggravating circumstances and applying mitigating factors not included in the agreement to initiate the procedure.

Among the aggravating circumstances that UST GLOBAL understands corrected, it mentions the serious diligence, linking the activity of the company with the processing of data in the workplace, which is denied by the claimed entity.

Also in relation to the aggravating circumstances, the respondent alleges that, if there was no intentionality or negligence, the sanction cannot be aggravated by a serious lack of diligence; nor for the consideration of the entity as a large company, indicated in the start-up agreement, or as a medium-sized company, as indicated in the proposal for

resolution, which is not among the aggravating or mitigating circumstances of the GDPR or the

LOPDGDD.

On the other hand, it stands out as mitigating factors valued in the proposal that they were not

considered at the beginning of the procedure those already indicated of absence of damages and the

environment in which the events take place (two people who worked together), the

measures taken by the company, the non-existence of personal data of category

special, or the absence of benefits.

Finally, it considers that it should be taken into account when setting the sanction that the entity

has DPD and the way in which the Agency has become aware of the facts,

through a claim by a former employee, eight months after leaving the

entity.

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited:

PROVEN FACTS

FIRST: The claimant served as an employee at the UST entity

GLOBAL. This entity has stated that the claimant was employed in the

same from 02/25/2019 to 04/03/2020

SECOND: UST GLOBAL, within the framework of the economic activity that it develops, was

contracted for the provision of services by the entity OpenBank.

THIRD: UST GLOBAL decided to incorporate the claimant, along with another employee

of that entity, to the management of the project that it developed as a service provider

from OpenBank.

FOURTH: On 01/08/2020, from the domain “@ust-global.com”, a message was sent

email addressed to two users with domain “@gruposantander.com”, with

copies three more users of the “@ust-global.com” domain, including the claimant and the

another is the employee of the claimed party to whom the content of the email refers. Is

communication has the subject "Access for new additions" and the following

text:

“Good morning… (names of Santander Group recipients)

Today we have incorporated two people to the OpenBank team, so we would need

that you request access to the VPN, Jira, etc.

The data is:

(…) (name and surname of the claimant, professional email address and

ID)

(...) (name and surname of another employee of the claimed, email address

professional e-mail and DNI).

According to UST GLOBAL, this email was sent by the supervisor of the

claimant.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of

control, and as established in arts. 47 and 48.1 of the LOPDGDD, the Director of

The Spanish Agency for Data Protection is competent to resolve this

process.

II

Previously, it is considered appropriate to analyze the formal issues raised

for the one claimed in its pleadings brief.

Both in its response to the opening of the procedure and the one presented on the occasion of the resolution proposal, the aforementioned entity alleges that the resolution of beginning of the sanctioning procedure can be annulled considering that in its Grounds of Law refers to a possible infringement of article 5.1.f) of the RGPD and in its operative part agrees to open proceedings for an alleged infringement of article 6 of the same Regulation, which has not been infringed.

In the opinion of this Agency, the start-up agreement issued is in accordance with the provisions of the Article 68 of the LOPDGDD, according to which it will suffice for said agreement to specify the facts that motivate the opening, identify the person or entity against which it is directed the procedure, the infraction that could have been committed and its possible sanction.

In the same sense, article 64.2 of the LPACAP is expressed, which establishes expressly the minimum content of initiation agreement. According to this precept, among other details, it must contain "the facts that motivate the initiation of the procedure, its possible legal qualification and the sanctions that could correspond, without prejudice to what results from the investigation".

In this case, not only are the aforementioned requirements amply met, but also the Legal Foundations of the repeated agreement goes further by offering reasoning that justifies the possible legal classification of the facts valued at beginning, mentioning, even, the circumstances that can influence the determination of the sanction.

In accordance with the foregoing, it cannot be said that the error made in the

dispositive of the agreement when pointing out the possible violation of article 6 of the RGPD, in

instead of article 5.1.f) of the same legal text referred to in the Foundations of

Law, has limited the defense possibilities of UST GLOBAL. this entity,

in this case, it has seen respected all the guarantees of the interested party that the

procedural regulations and it cannot be said that said error has led to any loss

of said guarantees causing defenselessness.

The respondent has known the possible classification of the facts and has been able to allege to the

respect in his defense what he has considered opportune. Proof of this is that there

made allegations about the non-violation of the provisions of article 5.1.f) of the

GDPR.

In accordance with the provisions of articles 89 and 90 of the LPACAP, they are the proposal of

resolution and the resolution those that fix the exact legal classification of the facts that

are considered proven.

III

Article 5 of the RGPD establishes the principles that must govern the treatment of personal data.

personal data and mentions among them that of “integrity and confidentiality”. East

Article, in section 1.f), states the following:

"1. The personal data will be:

(…)

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

including protection against unauthorized or unlawful processing and against loss,

accidental destruction or damage, through the application of technical or organizational measures appropriate (“integrity and confidentiality”)”.

Article 5 of the new Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter LOPDGDD), is refers to the “Duty of confidentiality” in the following terms:

"1. Those responsible and in charge of data processing, as well as all the people who intervene in any phase of this will be subject to the duty of confidentiality to which refers to article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary to the duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will be maintained even when the relationship of the obligor with the person responsible or in charge of the treatment had ended.

In the present case, the claimant was linked to the claimed as an employee, by virtue of an employment relationship.

Under that relationship, the claimant was assigned to the project that the claimed developed, as a service provider, for the entity OpenBank.

For this reason, the defendant communicated to OpenBank the personal data of the claimant regarding name and surname, professional email address and DNI, in order for the financial entity to arrange what is necessary to give the claimant access to the information system that would allow him to carry out the tasks that entail the provision of the service.

These processing of personal data of the claimant by the claimed, including the communication of those data to OpenBank, are deemed necessary for the compliance with the respective relationships that bind the participants in the facts.

However, said communication of data to the financial entity was made by

of the one claimed by email, dated 01/08/2020, in which no

only the indicated personal data relating to the claimant were included, but also

the data corresponding to another employee. This email was addressed to

OpenBank, but the recipients included the two employees holding the

transmitted data, so that each of them could have access to the data

of the other, according to the details that are outlined in the Proven Fact

Fourth.

This is a dissemination of personal data for which the claimed party does not have

legal basis that legitimizes it.

Consequently, the documentation in the file proves that the

claimed violated article 5 “Principles related to treatment” of the RGPD, section

1.f), in relation to article 5 “Duty of confidentiality” of the LOPGDD, having

sent an email that incorporated the personal identification data of

two interested parties, their email accounts and, especially, the DNI data,

allowing each of them to have knowledge of the data of the other.

This duty of confidentiality, previously the duty of secrecy, must be understood

whose purpose is to avoid those leaks of data not consented to by the users.

holders of them. This is an obligation incumbent on the controller and

in charge of the treatment, as well as anyone who intervenes in any phase of the

treatment; and that it is complementary to the duty of professional secrecy.

Faced with this non-compliance, it cannot simply oppose, as the

claimed in its allegations, the responsibility shown in compliance with the

personal data protection regulations. These are facts that

duly accredited, the scope and effect of which is expressed

previously.

The allegation made by the respondent to the proposal must also be rejected.

of resolution, when it states that the facts do not constitute a disclosure of data

given the work environment in which they occur; and considering it probable that

both partners were aware of the personal data of the other. Does not exist

no legal reason for a worker to have access to personal data

of another worker for the sole fact of belonging to the same organization

business; nor can the organization make them known to colleagues based on the

mere assumption that they are already known by them.

On the other hand, it is necessary to point out that it is not true what is indicated by the claimed in its

brief of arguments to the resolution proposal when pointing out that in this proposal

It has been considered that "the interested party has not suffered any damage or harm, both for

the data affected as by the framework in which they were shared" and that "it is about

two employees who work together and knew each other." These claims

appear in the Fifth Antecedent of the proposed resolution (also in the

this act), in which the allegations made by the entity

interested. Nothing to do with the factual and legal circumstances assessed for

determine the infraction or for the graduation of the sanction that is imposed.

IV

In the event that there is an infringement of the provisions of the RGPD, between the

corrective powers available to the Spanish Data Protection Agency,

as a control authority, article 58.2 of said Regulation contemplates the

following:

“2 Each control authority will have all the following corrective powers indicated below:

continuation:

(…)

b) send a warning to any person responsible or in charge of the treatment when the

treatment operations have violated the provisions of this Regulation;”

(...)

d) order the person responsible or in charge of the treatment that the treatment operations be

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

manner and within a specified time;

(…)

i) impose an administrative fine under article 83, in addition to or instead of the

measures mentioned in this section, according to the circumstances of each case

particular;".

According to the provisions of article 83.2 of the RGPD, the measure provided for in letter d)

above is compatible with the sanction consisting of an administrative fine.

v

In the present case, non-compliance with the provisions of the

article 5.1.f) of the RGPD, in relation to article 5 of the LOPDGDD, with the scope

expressed in the previous Fundamentals of Law, which supposes the commission of

an infringement typified in article 83.5.a) of the RGPD, which under the rubric

"General conditions for the imposition of administrative fines" provides what

Next:

“Infractions of the following provisions will be sanctioned, in accordance with section

2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of a company,

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

previous financial year, opting for the highest amount:

a) the basic principles for the treatment, including the conditions for the consent to

tenor of articles 5, 6, 7 and 9;”.

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

infractions the acts and behaviors referred to in sections 4, 5 and 6 of the

Article 83 of Regulation (EU) 2016/679, as well as those that are contrary to the

present organic law”.

For the purposes of the limitation period, article 72 of the LOPDGDD indicates:

“Article 72. Infractions considered very serious.

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

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

substance of the articles mentioned therein and, in particular, the following:

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

Article 5 of Regulation (EU) 2016/679”.

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

provisions of article 83, sections 1 and 2 of the RGPD, which indicate:

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

in accordance with this article for the infringements of this Regulation indicated in the

sections 4, 9 and 6 are in each individual case effective, proportionate and dissuasive.

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

individually, in addition to or as a substitute for the measures referred to in article 58,

section 2, letters a) to h) and j). When deciding to impose an administrative fine and its amount

In each individual case, due account shall be taken of:

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

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

such as the number of interested parties affected and the level of damages that

have suffered;

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

11/14

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor to

alleviate 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,

taking into account the technical or organizational measures that they have applied under

of 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, in what

measure;

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

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 mechanisms of

certification approved in accordance with article 42, and

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, through the infringement.

For its part, in relation to letter k) of article 83.2 of the RGPD, the LOPDGDD, in

its article 76, “Sanctions and corrective measures”, establishes:

"1. The sanctions 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 the

section 2 of the aforementioned article.

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

may be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the performance of data processing

personal.

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 crime.

infringement.

e) The existence of a merger by absorption process subsequent to the commission of the infraction,

that cannot be attributed to the absorbing entity.

f) Affectation of the rights of minors.

g) Have, when not mandatory, a data protection delegate.

h) Submission by the person in charge or person in charge, on a voluntary basis, to

alternative conflict resolution mechanisms, in those cases in which there are

controversies between them and any interested party”.

In this case, considering the concurrent circumstances, it is considered appropriate

the imposition of a fine. The request made by the respondent to

that other corrective powers be imposed, such as the warning, which is

provided for natural persons and when the sanction constitutes a burden

disproportionate (considering 148 of the RGPD).

In accordance with the precepts transcribed, in order to set the amount of the sanction of

fine to be imposed in the present case for the infraction typified in article 83.5.a)

of the RGPD, for which the claimed party is responsible, they are considered concurrent in

quality of aggravating the following factors that reveal a greater unlawfulness and/or

fault in the conduct of the entity claimed:

. The negligence appreciated in the commission of the infraction: there is no record

that the entity has acted maliciously, although the action reveals a

serious lack of diligence.

In relation to this circumstance, the respondent understands that the lack of diligence

cannot aggravate the sanction, considering that article 83.2 of the RGPD is

Refers to intent or negligence. In this regard, this Agency understands that

the indicated lack of diligence expresses a lack of care, assimilable in its

definition of the concept of negligence.

. The link between the activity of the offender and the performance of treatment of

personal data in the workplace.

Taking into account the number of people (689) who serve as

employees of UST GLOBAL, the link between this entity and the

processing of personal data in the indicated scope.

. The condition of medium-sized company of the responsible entity and its volume of business.

The respondent understands that this factor cannot be taken into consideration as it does not appear among the circumstances listed in the RGPD or the LOPDGDD. Without However, it does not take into account the provisions of letter k) of article 83.2 of the RGPD, that admits the assessment, for the purposes of grading the fine to be imposed, of "any other aggravating or mitigating factor applicable to the circumstances of the case."

. The categories of personal data affected by the infringement. In contrary to what is stated in the motion for a resolution, which values this circumstance As a mitigating factor, this Agency has repeatedly considered that the implication in the facts of identification data of the interested parties must be appreciated in the graduation of the sanction as an aggravating factor.

Likewise, the following circumstances are considered extenuating:

. The nature, seriousness and duration of the infringement: the infringement results from a isolated treatment operation of merely local scope.

. The offense is not ongoing.

. The low volume of data and processing that constitutes the object of the proceedings.

. The number of interested parties, given that they have only been affected by the conduct offending two people.

. The respondent entity has adopted measures to prevent the occurrence of

similar incidents, giving instructions to their units and through

training activities for its employees.

. The responsible entity has not obtained benefits as a result of the

commission of the offence.

The designation of DPO by the respondent is not considered mitigating,

that it is nothing but the fulfillment of a legal obligation; or the way in which the Agency

has become aware of the infringement, which took place through a claim from one

of those affected by the infringement, and not by direct communication from the person in charge.

Considering the exposed factors, especially, the measures taken during the

processing of the procedure to avoid similar incidents, it is considered appropriate

reduce the proposed sanction and impose a fine of 3,000 euros.

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of sanctions whose existence has been proven,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE UST GLOBAL ESPAÑA, S.A., with NIF A84816644, for a

infringement of article 5.1.f) of the RGPD, in relation to article 5 of the LOPDGDD,

typified in Article 83.5 of the RGPD, and classified as very serious for the purposes of

prescription in article 72 of the LOPDGDD, a fine amounting to 3,000 euros

(three thousand euros).

SECOND: NOTIFY this resolution to UST GLOBAL ESPAÑA, S.A.

THIRD: Warn the sanctioned party that he must make the imposed sanction effective once

Once this resolution is enforceable, in accordance with the provisions of the

art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (hereinafter LPACAP), within the payment term

voluntary established in art. 68 of the General Collection Regulations, approved

by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,

of December 17, through its entry, indicating the NIF of the sanctioned and the number

of procedure that appears in the heading of this document, in the account

restricted number ES00 0000 0000 0000 0000 0000, opened on behalf of the Agency

Spanish Department of Data Protection in the banking entity CAIXABANK, S.A.. In case

Otherwise, it will be collected in the executive period.

Received the notification and once executed, if the date of execution is

between the 1st and 15th of each month, both inclusive, the term to make the payment

voluntary will be until the 20th day of the following month or immediately after, and if

between the 16th and last day of each month, both inclusive, the payment term

It will be until the 5th of the second following month or immediately after.

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 in accordance with art. 48.6 of the

LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the

Interested parties may optionally file an appeal for reconsideration before the

Director of the Spanish Agency for Data Protection within a month from

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

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

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

the fourth additional provision of Law 29/1998, of July 13, regulating the

Contentious-administrative jurisdiction, within a period of two months from the

day following the notification of this act, as provided in article 46.1 of the

aforementioned Law.

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

may provisionally suspend the firm resolution in administrative proceedings if the

The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact by

writing addressed to the Spanish Agency for Data Protection, presenting it through

Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registers provided for in art. 16.4 of the

aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the

documentation proving the effective filing of the contentious appeal-

administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative within a period of two months from the day following the

notification of this resolution would end the precautionary suspension.

Sea Spain Marti

Director of the Spanish Data Protection Agency

938-131120

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es