

□ File No.: EXP202202150

## RESOLUTION OF SANCTIONING PROCEDURE

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

### BACKGROUND

FIRST: Ms. A.A.A. (hereinafter, the claiming party) dated January 11,  
2022 filed a claim with the Spanish Data Protection Agency. The  
claim is directed against DIGI SPAIN TELECOM, S.L. with NIF B84919760 (in  
forward, the claimed party or DIGI). The reasons on which the claim is based are the following:  
following:

The claimant states that on January 7, 2022 the service of its line  
phone \*\*\*PHONE.1 did not work, and the claimed party informed him that with his  
data a duplicate SIM card had been requested.

After the claimant informed during that call that she had not contacted  
DIGI, nor had requested the issuance of a duplicate of its SIM card, DIGI proceeded to  
cancel the issuance of the duplicate SIM, and restore the operation of the SIM  
original that was in the possession of the claimant.

Well, on January 9, 2022, he again ran out of a mobile line, for having  
requested a new duplicate SIM card for your mobile line

\*\*\*TELEPHONE 1.

Later, he was able to verify how the impersonator had entered his account  
bank, making use of it.

He filed a complaint with the Logroño National Police on January 8, 2022 and  
their corresponding extensions, in view of the events that occurred on the 9th of the same month  
not anymore.

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

December, Protection of Personal Data and guarantee of digital rights (in forward LOPDGDD), said claim was transferred to the claimed party, for 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 regulations of Data Protection.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of October 1, of the Common Administrative Procedure of the Administrations Public (hereinafter, LPACAP), was collected on February 21, 2022 as

It appears in the acknowledgment of receipt that is in the file.

On March 22, 2022, this Agency received a written response indicating that they have verified the existence of a duplicate SIM card request

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

2/17

relative to the claimant's mobile line. Said request, made on January 7, of 2022 was carried out through the channel that the customer service that DIGI has enabled via WhatsApp.

The aforementioned request was made by a person who identified himself as the claimant, providing your personal data and overcoming the security challenge established by DIGI in order to verify the identity of the client.

For security reasons they proceeded to the preventive blocking of the previous SIM card, since its theft had been alleged. The same day they received a telephone communication from the claimant alleging that her mobile line did not work, after that communication and the

verifications carried out proceeded to cancel the issuance process

duplicate SIM, and restore the operation of the original SIM that was in

power of the claimant. They proceeded to establish a warning note in the systems

regarding the fact that the claimant could be immersed in a case of usurpation of

identity.

It is stated that for customer service there is an obligation to

Consult customer history to avoid similar cases. It is pointed out that the

The measures adopted were adequate to be able to reject several attempts to

make a duplicate by the usurped.

However, it is stated that on January 9, 2022, in another attempt to obtain

duplicate, there was a human error in the customer service and that despite the

warning note, the necessary numerical code was provided to process the

duplicate SIM.

After a call from the claimant, that same day, they proceeded to deactivate said

duplicate.

The entity declares that it has not disclosed personal data of the company to any third party.

claimant, not knowing how the usurper could know his personal data

to overcome established security controls.

A series of measures were adopted:

Immediate rectification of the element causing the incident, canceling the issue

of the duplicate (on the first attempt because an error was made on the second and the

continuing process ahead).

The measures adopted by the person in charge to deal with situations are detailed.

of this type.

THIRD: On April 6, 2022, in accordance with article 65 of the

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

FOURTH: The General Subdirectorate of Data Inspection proceeded to carry out of previous investigative actions to clarify the facts in matter, 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)

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

3/17

2016/679 (General Data Protection Regulation, hereinafter GDPR), and in accordance with the provisions of Title VII, Chapter I, Second Section, of the LOPDGDD, having knowledge of the following extremes:

#### RESULT OF INVESTIGATION ACTIONS

(...)

FIFTH: On December 13, 2022, the Director of the Spanish Agency for Data Protection agreed to initiate disciplinary proceedings 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 (in hereinafter, LPACAP), for the alleged infringement of Article 6.1 of the GDPR, typified in Article 83.5 of the GDPR.

SIXTH: On December 27, 2023, DIGI requests the extension of the legal term conferred to answer said requirement and a copy of the file.

SEVENTH: On January 19, 2023, it is received at this Agency, on time and form, written by the representative of DIGI in which, in summary, it is argued that reiterate in the allegations previously presented, first pointing out that chronological manner in which the events occurred, indicating the security protocol and

the measures adopted for these events, stating that DIGI has not made available disposition of the alleged criminals personal information of the complainant different from what they already had before, after having obtained them through of the email.

Consequently, they point out that it is not possible to associate DIGI with carrying out a non-legitimized processing of personal data, given that its performance is reduced to compliance with its processes and obligations.

In other words, during the process of requesting and delivering the duplicate, a processing of personal data provided to DIGI in order for it to verify the identity of the interlocutor, first by telephone and later in person.

In addition, DIGI states that it is proven that identity theft and the illegitimate access to the claimant's data occurs through a phone call to customer service, prior to having contact with DIGI, the alleged impersonator had in his possession the personal data of the claimant, including his bank account (which also allowed him to access she).

On the other hand, it points out that the AEPD unequivocally imposes on DIGI a strict liability, in which, regardless of the diligence and measures deployed, the entity is found guilty. The AEPD seems to confuse the concept of proactive responsibility with the obligation of result imposed by the strict liability. In the present case, the existence of a strict control, before and after the application of the duplicate, the establishment of prior and subsequent measures, as well as the existence of measures aimed at Avoid these practices in advance.

For this reason, the claimed party considers that this Startup Agreement is not adjusted to law, since it imposes on DIGI an obligation of result, based on only in the harmful result that is produced by the fraudulent activity of a third, regardless of the diligence used and without considering the deployment of measures technically adequate and implemented.

In addition, it indicates that the following extenuating circumstances currently exist that have not been considered in the appropriate graduation of the sanction:

The absence of previous infringements committed by DIGI (art. 83.2 e) GDPR).

At no time have special categories of data been processed (Art. 83.2 g) GDPR)

The degree of cooperation of DIGI with the AEPD in order to remedy a alleged infringement and mitigate its possible adverse effects (art. 83.2 f) GDPR).

The non-existent benefit obtained (Art. 83.2 k).

It requests that a resolution be issued by means of which it indicates the file of the procedure.

Subsidiarily warning and, ultimately, moderate or modulate the proposal included in the Initiation Agreement

EIGHTH: On January 19, 2023, the instructor of the procedure agreed perform the following tests: 1. They are considered reproduced for probative purposes the claim filed by Ms. A.A.A. and its documentation, the documents obtained and generated during the phase of admission to processing of the claim, and the report of previous investigation actions that are part of the procedure.

2. Likewise, it is considered reproduced for evidentiary purposes, the allegations to the agreement initiation of the referenced sanctioning procedure, presented by DIGI SPAIN TELECOM, S.L., and the documentation that accompanies them.

NINTH: On February 13, 2023, a resolution proposal was formulated, proposing that the Director of the Spanish Data Protection Agency sanction DIGI SPAIN TELECOM, S.L., with NIF B84919760, for an infringement of the Article 6.1 of the GDPR, typified in Article 83.5 a) of the GDPR, the sanction that would correspond would be a fine for an amount of 70,000 euros (seventy thousand euros).

TENTH: Once the proposed resolution was notified, the defendant requested an extension term to formulate allegations that was granted, presented a brief of allegations on March 6, 2023 in which, in summary, it is argued that it is reiterated in the allegations previously presented, and that in the report issued by the Agency of Cybersecurity of the European Union ratifies that, to make a duplicate SIM fraud, the fraudster needs to have access to some of the data personal data of the victim, client of the operator. That is, that cybercriminals, have personal data of their victims prior to going before the Mobile Network Operator.

He points out that this is what happened in this case, the victim lost control about your personal data in favor of the impersonator prior to the latter contact DIGI. That is, it is through the "phishing" attack where the victim

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

5/17

lose control over your personal data, and it is this fact that

triggers and enables the commission of fraud.

Likewise, it states that it must be taken into account that DIGI does not participate in the process of identification of a user before his bank, but rather the latter who determines the way in which you want to carry out this check, so it is not possible to move the liability to telephone operators.

Likewise, they indicate that it is for this reason that the defendant considers that the Proposal is not adjusted to law, since it imposes on DIGI an obligation of result, consisting of the establishment of infallible measures, when imputing a violation of the Article 6.1 of the GDPR based solely on the harmful result that occurs due to the fraudulent intervention of a third party, regardless of the diligence used and without consider the deployment of technically adequate and implemented measures.

DIGI cannot anticipate or know what the applicable duty of care is.

On the lack of proportionality of the proposed sanction and that prior to the procedures timely, a resolution is issued by means of which the file of the procedure is indicated No. EXP202202150.

Of the actions carried out in this procedure and of the documentation in the file, the following have been accredited:

#### PROVEN FACTS

FIRST. - The claimant filed a claim with this Agency on the 11th of January 2022, in which it is stated that on January 7, 2022, the service of the claimant's mobile line was not working, and was informed by DIGI that a request had been made a duplicate of the SIM card of your mobile line. DIGI canceled the issuance of the aforementioned duplicate, and proceeded to establish a warning note in the systems on that day regarding the fact that the claimant could be immersed in a case of usurpation of identity.

On January 9, 2022, he again lost service on his mobile line, due to



have requested a new duplicate of your SIM card and the impersonator entered your bank account, making use of it.

SECOND. - DIGI certifies that the claimant was left without a mobile line on the days January 7 and 9, 2022. It is clear that on January 7 DIGI canceled the issuance of the duplicated and alerted of said circumstance in their systems.

THIRD. - DIGI accredits the following incidents on January 9, 2022:

- Chat corresponding to the security challenge of a request attempt from 9 January 2022 at 5:26 p.m., in which Customer Service indicates that it is not possible to proceed in this way to manage the request and that you must send identity document to carry it out, stating the representatives of the

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

6/17

claimed part that was rejected due to the existence of a previous entry in the history of the phishing client.

- A third party contacted your customer service on January 9, 2022. client, by telephone, requesting the issuance of a duplicate SIM card of the claimant and proceeded to issue a duplicate request code of the SIM card, that same day the third one showed up at a distribution point from DIGI. There they proceeded to issue the SIM card to said third party who was not the owner of the line, and that on this occasion there was a human error due to the telephone advisor, which, despite the warning note reflected in the systems and after providing the alleged usurper with the necessary data to overcome the security challenge authorized the duplicate SIM card.

ROOM. - The duplicate was issued at a DIGI dealer location, the on January 9, 2022 at 6:46 p.m., and when the claimant contacted the customer service, DIGI proceeded to deactivate the duplicate SIM fraudulent and the next day the claimant contacted the company to request the Unsubscribe from all your services.

## 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: "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

The claimed party is accused of committing an offense for violation of the Article 6 of the GDPR, "Legacy of the treatment", which indicates in its section 1 the cases in which the processing of third-party data is considered lawful:

"1. Processing will only be lawful if at least one of the following is fulfilled

conditions:

a) the interested party gave his consent for the processing of his personal data

for one or more specific purposes;

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

7/17

b) the treatment is necessary for the execution of a contract in which the interested party

is part of or for the application at the request of the latter of pre-contractual measures;

c) the processing is necessary for compliance with a legal obligation applicable to the responsible for the treatment;

d) the processing is necessary to protect vital interests of the data subject or of another

Physical person;

e) the treatment is necessary for the fulfillment of a mission carried out in the interest

public or in the exercise of public powers conferred on the data controller;

f) the treatment is necessary for the satisfaction of legitimate interests pursued

by the person in charge of the treatment or by a third party, provided that on said

interests do not outweigh the interests or fundamental rights and freedoms of the

interested party that require the protection of personal data, in particular when the

interested is a child. The provisions of letter f) of the first paragraph shall not apply.

application to processing carried out by public authorities in the exercise of their

functions”.

Classification and classification of the offense

II

The infringement is typified in article 83.5 of the GDPR, which considers as such:

"5. Violations of the following provisions will be penalized, in accordance with the section 2, with administrative fines of a maximum of 20,000,000 EUR 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:

a) The basic principles for the treatment, including the conditions for the consent in accordance with articles 5,6,7 and 9."

The LOPDGD, for the purposes of the prescription of the infringement, qualifies in its article 72.1 very serious infringement, in this case the limitation period is three years, "b)

The processing of personal data without the fulfillment of any of the conditions of legality of the treatment established in article 6 of Regulation (EU) 2016/679".

In response to the allegations presented by the respondent entity, it should be noted the next:

Regarding the fact that DIGI has not made available to the alleged criminals personal information of the complaining party other than that already held by those with anteriority. Consequently, there has been no unauthorized treatment of personal information.

Indeed, the issuance of a duplicate is not enough to carry out operations bank accounts on behalf of the holders, certainly, to complete the scam, it is necessary for a third party to "supplant the identity" of the owner of the data before the entity financial.

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

What entails a priori, a treatment outside the principle of legality because a third party is processing data, since it has access to them, without any legal basis, in addition of the violation of other principles such as confidentiality.

For this reason, this is a process where the diligence provided by the operators is essential to avoid this type of scam and violation of the GDPR.

Diligence that translates into the establishment of adequate measures to guarantee that the data processing is in accordance with the GDPR.

Identical considerations deserve the actions of banking entities that provide payment services, in which area this type of scam starts, since the third party has access to the affected user's credentials and poses as this.

While these entities are responsible for the processing of the data of their customers, they are responsible for the same obligations as those indicated up to now for the operators referring to compliance with the RGPD and the LOPDGDD, and also the derived from Royal Decree-Law 19/2018, of November 23, on payment services and other urgent financial measures.

It can be inferred that DIGI has provided a duplicate SIM card to a third party other than the legitimate owner of the mobile line, after overcoming by a third party the policy of existing security, which shows a breach of the duty to protect the customer information.

Denying the concurrence of a negligent act on the part of DIGI would amount to recognize that their conduct -by action or omission- has been diligent. Obviously not

We share this perspective of the facts, since the

lack of due diligence. It is very illustrative, the SAN of October 17, 2007

(rec. 63/2006), assuming that these are entities whose activity involves

in continuous treatment of customer data, indicates that "...the Supreme Court comes

understanding that imprudence exists whenever a legal duty of care, that is, when the offender does not behave with the required diligence. And in the assessment of the degree of diligence, professionalism must be especially considered or not of the subject, and there is no doubt that, in the case now examined, when the The appellant's activity is constant and abundant handling of personal data. staff must insist on rigor and exquisite care in adjusting to the legal provisions in this regard.

It is proven in the file that security has not been guaranteed appropriate in the processing of personal data, taking into account the result that identity theft has occurred. That is, a third party has managed to access to the personal data of the owner of the line.

Regarding the fact that criminals have not managed to obtain personal data from DIGI, so there can be no talk of breach of protection measures, point out that access to a duplicate SIM card that makes its user identifiable owner, responds to the definition of personal data in article 4.1) of the GDPR.

Regarding the responsibility of DIGI, it should be noted that, in general, DIGI [www.aepd.es](http://www.aepd.es)

C / Jorge Juan, 6

28001 – Madrid

[sedeagpd.gob.es](http://sedeagpd.gob.es)

9/17

processes the data of its clients under the provisions of article 6.1 b) of the GDPR, as it is considered a necessary treatment for the execution of a contract in which the interested party is part or for the application at his request of measures pre-contractual In other cases, it bases the legality of the treatment on the bases provided for in article 6.1.a), c), e) and f) of the GDPR.

On the other hand, to complete the scam, it is necessary for a third party to "impersonate the identity" of the owner of the data, to receive the duplicate of the SIM card. Which entails a priori, a treatment outside the principle of legality since a third party is processing data, since it has access to them, without any legal basis, in addition to the violation of other principles such as confidentiality.

Certainly, the principle of responsibility provided for in article 28 of the LRJSP, provides that: "They may only be penalized for acts constituting an infringement administrative authority for natural and legal persons, as well as when a Law recognize capacity to act, affected groups, unions and entities without legal personality and independent or autonomous estates, which result responsible for them by way of fraud or negligence."

However, the mode of attribution of liability to legal persons is not corresponds to the willful or reckless forms of guilt that are imputable to human behavior. So, in the case of offenses committed by legal persons, even if the element of guilt must be present, it will be necessarily applies differently from what is done with respect to persons physical.

According to STC 246/1991 "(...) this different construction of the imputability of self-

The infringement of the legal entity arises from the very nature of legal fiction to which these subjects respond. The volitional element in the strict sense is lacking in them. to, but not the ability to break the rules to which they are subject.

Infringement capacity and, therefore, direct reproach that derives from the good protected by the rule being infringed and the need for such protection is really effective and because of the risk that, consequently, the person must assume that is subject to compliance with said standard" (in this sense STS of 24 November 2011, Rec 258/2009).

To the foregoing must be added, following the judgment of January 23, 1998, partially transcribed in the SSTs of October 9, 2009, Rec 5285/2005, and of 23 of October 2010, Rec 1067/2006, that "although the guilt of the conduct must also be the object of proof, must be considered in order to assume the corresponding charge, which ordinarily the volitional and cognitive elements necessary to appreciate it are part of the typical behavior tested, and that its exclusion requires that the absence of such elements be proven, or in its aspect regulations, that the diligence that was required by the person claiming their nonexistence; In short, it is not enough to exculpate a behavior the invocation of the absence of guilt is typically unlawful".

Accordingly, the plea is dismissed. ultimate responsibility on the treatment continues to be attributed to the person in charge, who is the one who determines the

[www.aepd.es](http://www.aepd.es)

C / Jorge Juan, 6

28001 – Madrid

[sedeagpd.gob.es](http://sedeagpd.gob.es)

10/17

existence of the treatment and its purpose. Let us remember that, in general, the operators process the data of their customers under the provisions of article 6.1 b) of the GDPR, as it is considered a necessary treatment for the execution of a contract in which the interested party is a party (...). In this sense, DIGI has a network of sales representatives, points of sale and authorized distributors through a distribution contract to offer DIGI services. Among these services offered from their points of sale, is making duplicate SIM cards corresponding to a mobile telephone line.

Regarding the breach of the principle of proportionality, the GDPR provides



expressly the possibility of graduation, through the provision of fines subject to modulation, in response to a series of circumstances of each case individual.

Regarding the imposition of a warning, warning, or the adoption of corrective measures pursuant to article 58 of the GDPR, a deterrent fine is one that has a genuine deterrent effect. In this regard, the Judgment of the CJEU, of June 13, 2013,

C-511/11,

ECLI:EU:C:2013:386, says:

Versalis Spa v Commission,

“ 94. Regarding, firstly, the reference to the Showa Denko v Commission judgment, quoted above, it should be noted that Versalis interprets it incorrectly. Indeed, the Court of Justice, when stating in section 23 of said judgment that the factor deterrent is assessed taking into consideration a multitude of elements and not only the particular situation of the company in question, referred to points 53 to 55 of the conclusions presented in that case by Advocate General Geelhoed, who had stated, in essence, that the deterrent multiplier factor may be aimed at not only "general deterrence", defined as an action to discourage all companies, in general, from committing the infringement of in question, but also a "specific deterrence", consisting of dissuading the particular defendant so that he does not break the rules again in the future. For the Therefore, the Court of Justice only confirmed, in that judgment, that the Commission did not was required to limit its assessment to factors related solely to the particular situation of the company in question.”

“102. According to settled case law, the objective of the dissuasive multiplying factor and consideration, in this context, of the size and overall resources of the

company in question lies in the desired impact on said company, since the sanction should not be insignificant, especially in relation to the ability of the company (in this sense, see, in particular, the judgment of 17 June 2010, *Lafarge v Commission*, C-413/08 P, ECR p. I-5361, section 104, and the writ of February 7, 2012, *Total and Elf Aquitaine v Commission*, C-421/11 P, paragraph 82).

We must attend to the singular circumstance of the claim presented, through from which it can be seen that, from the moment the person impersonator performs the SIM replacement, the victim's phone is left without service passing control of the line to the impersonators. Consequently, their powers of disposal and control over their personal data are affected, which constitute part of the content of the fundamental right to data protection as indicated by the Constitutional Court in Judgment 292/2000, of 30 November 2000 (FJ 7). So, when getting a duplicate SIM card,

[www.aepd.es](http://www.aepd.es)

C / Jorge Juan, 6

28001 – Madrid

[sedeagpd.gob.es](http://sedeagpd.gob.es)

11/17

Under certain circumstances, access to the contacts or the applications and services that have as a key recovery procedure the sending an SMS with a code to be able to modify the passwords. Definitely, may impersonate the identity of those affected, being able to access and control, for example: email accounts; bank accounts; apps like WhatsApp; social networks, such as Facebook or Twitter, and a long etc. in short accounts, once the password has been modified by the impersonators, they lose control of your accounts, applications and services, which poses a great threat.

In short, it is the data controller who has the obligation to integrate the necessary guarantees in the treatment, with the purpose of, by virtue of the principle of proactive responsibility, comply and be able to demonstrate compliance, at the same while respecting the fundamental right to data protection.

In the present case, it is proven that on January 7 and 9, 2022 DIGI processed the issuance of duplicate SIM cards for line \*\*\*TELEFONO.1, belonging to the complaining party.

However, it should be noted that Sim Swapping is a fraud that allows you to impersonate identity by kidnapping the phone number by obtaining a duplicate of the SIM card.

In any case, the operator must be able to prove that for this specific case have followed the verification protocols implemented when requesting a duplicate SIM card.

Well then, the result was that the defendant issued the SIM card to a third party who did not he was the owner of the line.

In view of the foregoing, DIGI is unable to prove that this procedure.

In fact, according to the identification procedure described by the defendant, the original of the identification document should have been checked, whereas, otherwise If this operation had been carried out correctly, the duplicate should have been denied.

Well, between the two issued duplicates, another authorization attempt was rejected of duplicates through the channel that DIGI customer service has enabled via WhatsApp. However, despite the existence of the annotation of notice the second duplicate dated January 9, 2022 was authorized due to human error of the manager. In any case, the claimed party has not been able to prove that for

In this case, the procedure implemented by itself was followed, since, otherwise, to have done so, the duplicate card denial should have occurred  
SIM.

Based on the foregoing, in the case analyzed, the diligence used by the defendant to identify the person who requested a duplicate SIM card.

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

12/17

Based on the available evidence, it is estimated that the conduct of the claimed party violates article 6.1 of the GDPR and may be constitutive of the infringement typified in article 83.5.a) of the aforementioned Regulation 2016/679.

In this sense, Recital 40 of the GDPR states:

"(40) For processing to be lawful, personal data must be processed with the consent of the interested party or on some other legitimate basis established in accordance a Law, either in this Regulation or under other Union law or of the Member States referred to in this Regulation, including the the need to comply with the legal obligation applicable to the data controller or the need to execute a contract to which the interested party is a party or for the purpose of take measures at the request of the interested party prior to the conclusion of a contract."

Fine sanction. Determination of the amount.

IV.

The determination of the sanction that should be imposed in the present case requires

observe the provisions of articles 83.1 and 2 of the GDPR, precepts that,

respectively, provide the following:

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

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

have suffered;

b) intentionality or negligence in the infraction;

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;

[www.aepd.es](http://www.aepd.es)

C / Jorge Juan, 6

28001 – Madrid

[sedeagpd.gob.es](http://sedeagpd.gob.es)

- 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 extent;
- i) when the measures indicated in article 58, paragraph 2, have been ordered 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. fictions approved in accordance with article 42, and
- 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.”

Within this section, the LOPDGDD contemplates in its article 76, entitled "Sancio- and corrective measures":

"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) The link between the activity of the offender and the performance of data processing. personal information.
- 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 by absorption process subsequent to the commission of the violation, 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) Submission by the person responsible or in charge, on a voluntary basis, to alternative conflict resolution mechanisms, in those cases in which there are controversies between those and any interested party.

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

14/17

3. It will be possible, complementary or alternatively, the adoption, when appropriate, of the remaining corrective measures referred to in article 83.2 of the Regulation (EU) 2016/679.”

Digi requests that the following extenuating circumstances be appreciated:

(I) "the absence of prior infringements" (art. 83.2 e) GDPR).

(II) "At no time have special categories of data been processed" (art. 83.2 g).

(III) "cooperation with the supervisory authority in responding to the transfer of the claim and having provided the requested information", article 83.2 f) of the GDPR.

(IV) "The non-existence of benefits obtained through the infringement", article 83.2 k) of the GDPR and 76.2 c) of the LOPDGDD.

None of the invoked mitigations are allowed.

Regarding (I) and (II), it should be noted that such circumstances can only operate as aggravating and in no case as mitigating.

The pronouncement made by the National Court in its SAN of May 5, 2021

(Rec. 1437/2020) on section e) of article 83.2. of the GDPR, the commission of

previous violations:

"Considers, on the other hand, that the non-commission should be considered as mitigating

from a previous violation. Well, article 83.2 of the GDPR establishes that

must be taken into account for the imposition of the administrative fine, among

others, the circumstance "e) any previous infringement committed by the person responsible or

the person in charge of the treatment". This is an aggravating circumstance, the fact

The fact that the budget for its application does not meet implies that it cannot be

taken into consideration, but does not imply or allow, as the plaintiff claims,

its application as a mitigation";

(III) Article 83.2.f) of the GDPR refers to the "degree of cooperation with the

control in order to remedy the infringement and mitigate the possible effects

adverse effects of the offence;". The respondent's response to the information request

of the Sub-directorate of Inspection did not meet these purposes, so it is not

framed in that mitigation.

(IV) On the application of article 76.2.c) of the LOPDGDD, in connection with the

Article 83.2.k), non-existence of benefits obtained, it should be noted that such

circumstance can only operate as an aggravating circumstance and in no case as a mitigating circumstance.

Article 83.2.k) of the GDPR refers to "any other aggravating or mitigating factor

applicable to the circumstances of the case, such as the financial benefits obtained or the

losses avoided, directly or indirectly, through the breach." and the article

76.2c) of the LOPDGDD says that "2. In accordance with the provisions of article 83.2.k) of the

Regulation (EU) 2016/679 may also be taken into account: [...] c) The benefits

obtained as a consequence of the commission of the infraction." Both provisions

mentioned as a factor that can be taken into account in grading the sanction



the “benefits” obtained, but not the “absence” of these, which is what DIGI claims.

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

15/17

In addition, in accordance with article 83.1 of the GDPR, the imposition of fine sanctions is governed by the following principles: they must be individualized for each particular case, be effective, proportionate and dissuasive. The admission that it operates as a mitigation, the absence of benefits is contrary to the spirit of article 83.1 of the GDPR and the principles governing the determination of the amount of the fine penalty. If, as a result of the commission of a violation of the GDPR, it is classified as mitigating the fact that there have been no benefits, the dissuasive purpose that it is fulfilled through the sanction. Accepting DIGI's thesis in a case such as the one we are dealing with would mean introducing an artificial reduction in the penalty that truly it should be imposed; the one that results from considering the circumstances of article 83.2 GDPR that must be valued.

The Administrative Litigation Chamber of the National Court has warned that the fact that in a specific case not all the elements that constitute a circumstance modifying liability that, by its nature, has an aggravating nature, cannot lead to the conclusion that said circumstance is applicable as a mitigation. The pronouncement made by the National Court in its SAN of May 5, 2021 (Rec. 1437/2020) -even though that resolution is seen on the circumstance of section e) of article 83.2. of the GDPR, the commission of previous infractions - can be extrapolated to the question raised, the claim of the demanded that the "absence" of benefits be accepted as mitigation, thus

that both the GDPR and the LOPDGDD refer only to "the benefits obtained":

"Considers, on the other hand, that the non-commission should be considered as mitigating from a previous violation. Well, article 83.2 of the GDPR establishes that must be taken into account for the imposition of the administrative fine, among others, the circumstance "e) any previous infringement committed by the person responsible or the person in charge of the treatment". This is an aggravating circumstance, the fact The fact that the budget for its application does not meet implies that it cannot be taken into consideration, but does not imply or allow, as the plaintiff claims, its application as a mitigation";

In accordance with the precepts transcribed, for the purpose of setting the amount of the sanction of fine to be imposed on the entity claimed as responsible for a classified offense in article 83.5.a) of the GDPR and 72.1 b) of the LOPDGDD, are considered concurrent in the present case the following factors:

As aggravating factors:

-

The evident link between the business activity of the defendant and the treatment of personal data of clients or third parties (article 83.2.k, of the GDPR in relation to article 76.2.b, of the LOPDGDD).

The Judgment of the National Court of 10/17/2007 (rec. 63/2006), in which, with respect to entities whose activity entails the continuous processing of customer data, indicates that "...the Supreme Court has understood that recklessness exists whenever a legal duty of care is neglected, that is that is, when the offender does not behave with the required diligence. And in the assessment of the degree of diligence, special consideration must be given to the professionalism or not of the subject, and there is no doubt that, in the case now examined, when the appellant's activity is constant and abundant

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](http://sedeagpd.gob.es)

16/17

handling of personal data must insist on rigor and exquisite

Be careful to comply with the legal provisions in this regard.”

As mitigations:

The claimed party proceeded to resolve the incident that is the subject of the claim

effective (art. 83.2 c).

The balance of the circumstances contemplated in article 83.2 of the GDPR, with

regarding the offense committed by violating the provisions of article 6.1 of the

GDPR allows a penalty of 70,000 euros (seventy thousand euros) to be set.

Therefore, in accordance with the applicable legislation and assessed the criteria of

graduation of sanctions whose existence has been accredited, the Director of the

Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE DIGI SPAIN TELECOM, S.L., with NIF B84919760, for a

violation of Article 6.1 of the GDPR, typified in Article 83.5 of the GDPR, a fine

of 70,000 euros (seventy thousand euros).

SECOND: NOTIFY this resolution to DIGI SPAIN TELECOM, S.L.

THIRD: Warn the penalized person that they must make the imposed sanction effective

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

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

Common of Public Administrations (hereinafter LPACAP), within the payment period

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, by means of its income, indicating the NIF of the sanctioned and the number of procedure that appears in the heading of this document, in the account restricted IBAN number: ES00-0000-0000-0000-0000, open in the name of the Spanish Agency for Data Protection at the bank CAIXABANK, S.A..

Otherwise, it will proceed to its collection in the executive period.

Once the notification has been received and once executed, if the execution date 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 or immediately following business month, and if between the 16th and the last day of each month, both inclusive, the payment term It will be until the 5th of the second following or immediately following business month.

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 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 reversal before the

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

[www.aepd.es](http://www.aepd.es)

C / Jorge Juan, 6

28001 – Madrid

[sedeagpd.gob.es](http://sedeagpd.gob.es)

17/17

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.

Finally, it is noted 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 through

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

of the Electronic Registry of the Agency [[https://sedeagpd.gob.es/sede-electronica-](https://sedeagpd.gob.es/sede-electronica-web/)

web/], or through any of the other registries 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 proceedings within a period of two months from the day following the

Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

C / Jorge Juan, 6

28001 – Madrid

[www.aepd.es](http://www.aepd.es)

[sedeagpd.gob.es](https://sedeagpd.gob.es)