 File No.: PS/00194/2022

RESOLUTION OF SANCTIONING PROCEDURE

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

BACKGROUND

FIRST: Don A.A.A. (hereinafter, the claiming party), dated ***DATE.1, filed a claim with the Spanish Data Protection Agency (hereinafter, AEPD). The reasons on which the claim is based are the following:

The complaining party reports that several media outlets published on their websites the audio of the statement before the judge of a victim of a rape multiple, to illustrate the news regarding the holding of the trial in a case that was very mediatic The complaining party provides the links to the news published in the claimed media websites.

On ***DATE.2, a new letter sent by the complaining party is received stating that he has been able to verify that there are means that have eliminated that information, although it accompanies publications made by some media communication on Twitter where it is still available.

SECOND: On ***DATE.3, the claim submitted was admitted for processing by the complaining party.

THIRD: The General Subdirectorate of Data Inspection proceeded to carry out of previous investigative actions to clarify the facts in matter, by virtue of the investigative powers granted to the authorities of control in article 58.1 of Regulation (EU) 2016/679 (General Regulation of Data Protection, hereinafter GDPR), and in accordance with the provisions of the Title VII, Chapter I, Second Section, of the LOPDGDD, being aware of the

following extremes:

During the investigation actions, publications were found, more than

those initially denounced by the complaining party, where the voice of the complainant could be heard

undistorted victim. Among them, the following DISPLAY publication

CONNECTORS, S.L., with NIF B65749715 (hereinafter, the claimed party):

***URL.1

On ***DATE.4, the defendant was notified of a precautionary withdrawal measure

urgent content or distorted voice of the intervener in such a way that

will be unidentifiable in the web addresses from which this was accessible

content.

On ***DATE.5, this Agency receives a letter sent by the party

claimed informing that the news has been removed as soon as they have had

knowledge of the withdrawal request, verifying said circumstance

FOURTH: On April 28, 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 5.1.c) of the GDPR, classified as

in Article 83.5 a) of the GDPR.

FIFTH: Notified of the aforementioned start-up agreement in accordance with the rules established in

the LPACAP and after the period granted for the formulation of allegations, it has been

verified that no allegation has been received by the claimed party.

Article 64.2.f) of the LPACAP -provision of which the claimed party was informed

in the agreement to open the procedure - establishes that if no

arguments within the established term on the content of the initiation agreement, when

it contains a precise pronouncement about the imputed responsibility,

may be considered a resolution proposal.

In the present case, the agreement to initiate the sanctioning file determined the

facts in which the accusation was specified, the infringement of the GDPR attributed to the

claimed and the sanction that could be imposed. Therefore, taking into consideration that

the claimed party has not made allegations to the agreement to start the file and

In accordance with the provisions of article 64.2.f) of the LPACAP, the aforementioned agreement of

beginning is considered in the present case resolution proposal.

SIXTH: The agreement to initiate the procedure agreed in the third point of the part

dispositive "INCORPORATING into the disciplinary file, for evidentiary purposes, the

claim filed by the claimant and its documentation, as well as the

documents obtained and generated by the Sub-directorate General of Inspection of

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

In view of all the proceedings, by the Spanish Agency for Data Protection

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: On ***DATE.1, the claimant filed a claim with the

Spanish Agency for Data Protection denouncing that various media

communication published on their websites the audio of the statement before the judge of

a victim of a multiple rape, to illustrate the news regarding the celebration

of the trial in a case that was highly publicized, providing links to the news

published on the websites of the claimed media.

On ***DATE.2, a new letter sent by the complaining party is received

stating that he has been able to verify that there are means that have eliminated that

information, although it accompanies publications made by some media

communication on Twitter where it is still available.

SECOND: On ***DATE.3 the claim presented by

the complaining party.

THIRD: The General Sub-directorate of Data Inspection, in the exercise of its

investigative activities, found a publication of the Respondent where

could hear the victim's voice undistorted at the following address:

***URL.1

FOURTH: The person responsible for said publication is DISPLAY CONNECTORS, S.L. with

NIF B65749715. Consequently, it has been proven that the claimed party

published, on the aforementioned website, the audio of the statement before the judge

of the victim of a multiple rape, to illustrate the news regarding the celebration

of the trial in a case that was highly mediated.

FIFTH: On ***DATE.4, the defendant was notified of a precautionary measure

urgent removal of content or distorted voice of the victim in such a way that

will be unidentifiable in the web addresses from which this was accessible

content, specifically:

***URL.1

SIXTH: On ***DATE.5, a document sent by the Agency is received by this Agency.

claimed party informing that the news has been removed as soon as they have

had knowledge of the withdrawal request, verifying said

circumstance.

SEVENTH: The Spanish Data Protection Agency has legally notified

the party claimed the agreement to open this disciplinary proceeding,

but it has not presented allegations or evidence that contradict the facts

denounced.

FUNDAMENTALS OF LAW

Yo

Competence

By virtue of the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter GDPR) recognizes 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

The voice as personal data

The voice of a person, according to article 4.1 of the GDPR, is personal data

make it identifiable, and its protection, therefore, is the subject of said GDPR:

"Personal data": any information about an identified natural person or

identifiable ("the data subject"); An identifiable natural person shall be considered any person

whose identity can be determined, directly or indirectly, in particular by means of

an identifier, such as a name, an identification number, data of

location, an online identifier or one or more elements of identity

physical, physiological, genetic, mental, economic, cultural or social of said person;"

The voice is a personal and individual attribute of each physical person that is defined

for its height, intensity and timbre. Endowed with unique and singular distinctive features that

individualize it directly, associating it with a specific individual, it is molded

when speaking, being able to know, through it, the age, sex, state of health of the

individual, his way of being, his culture, his origin, his hormonal, emotional and

psychic. Elements of the expression, the idiolect or the intonation, are also data of

personal character considered together with the voice.

For this reason, report 139/2017 of the Legal Office of this Agency states that "the

image as well as the voice of a person is personal data, as will be

any information that makes it possible to determine, directly or indirectly, your identity

(…)"

In fact, the National Court Judgment dated March 19, 2014 (rec.

176/2012) says that "the voice of a person constitutes data of a personal nature, as

as can be deduced from the definition offered by article 3.a) of the LOPD,

as

<<any information concerning natural persons identified or

identifiable>>, an issue that is not controversial."

Article 4.2 of the GDPR defines "processing" as: "any operation or set of

of operations carried out on personal data or sets of personal data,

whether by automated procedures or not, such as the collection, registration,

organization, structuring, conservation, adaptation or modification, extraction,

consultation, use, communication by transmission, diffusion or any other form of

authorization of access, collation or interconnection, limitation, deletion or destruction."

The inclusion of a person's voice in journalistic publications, which identifies or

makes a person identifiable, implies a processing of personal data and, therefore,

Therefore, the person responsible for the treatment that carries out the same is obliged to comply with

the obligations for the data controller set forth in the GDPR and in

the LOPDGDD.

II

Right to data protection

This procedure is initiated because the claimed party published, on the website

referred to in the facts, the audio of the statement before the judge of a victim of a

multiple rape, to illustrate the news regarding the holding of the trial in a case

that was very mediatic. The victim's voice was clearly appreciated when recounting

with all the crudeness of details the multiple rape suffered. All this constitutes a

processing of personal data of the victim.

People have the power of disposal over their personal data, including

his voice, as well as its diffusion, resulting, without a doubt, deserving of

protection of the person whose personal data is disclosed in violation of the law

legal.

Thus, STC 292/2000, of November 30, provides that "the content of the right

Fundamental to data protection consists of a power of disposal and control

on personal data that empowers the person to decide which of those data

provide to a third party, be it the State or an individual, or which can this third party

collect, and which also allows the individual to know who owns that personal data

and for what, being able to oppose that possession or use. These powers of disposition and

control over personal data, which constitute part of the content of the right

fundamental to data protection are legally specified in the power to

consent to the collection, obtaining and access to personal data, its subsequent

storage and treatment, as well as its use or possible uses, by a third party, be it the

state or an individual. And that right to consent to knowledge and treatment,

computerized or not, of personal data, requires as complements

essential, on the one hand, the ability to know at all times who has

these personal data and to what use you are submitting them, and, on the other hand, the power

oppose such possession and uses".

In this sense, and regardless of the legal basis legitimizing the

treatment, all controllers must respect the principles of

treatment included in article 5 of the GDPR. We will highlight article 5.1.c) of the

GDPR which establishes that:

"1. Personal data will be

c) adequate, pertinent and limited to what is necessary in relation to the purposes for which

that are processed ("data minimization");"

However, we are faced with a fundamental right that is not absolute,

since, if necessary, the Fundamental Right to Data Protection can

give in to the prevalence of other rights and freedoms also constitutionally

recognized and protected, such as, for example, the Fundamental Right to Freedom of

Information, weighing it on a case-by-case basis.

However, in the present case, as we will explain, it must be considered that the

treatment carried out by the claimed party within the framework of the freedom of

information has been excessive, as there is no prevailing public interest in information in

the dissemination of the voice of the victim - without adding any added value to the information

keeping the real voice of the victim (without distorting, for example)-, under whose pretext

it seems that those data have been disclosed; voice that, added to the fact that it is

a highly publicized case, makes the victim clearly identifiable. By pondering the

conflicting interests and, considering the concurrent circumstances of this case,

that is, the especially sensitive nature of personal data and the intense

affectation of the privacy of the victim, the interest of the owner deserves greater protection

of the right to the protection of your personal data and that they are not disclosed in front of the

claimed public interest in its dissemination.

IV.

Information right

In the struggle between the Fundamental Rights to Freedom of Information in

relation to the Fundamental Right to the Protection of Personal Data, even

when an equal degree of protection is recognized for both constitutional rights,

ordinarily the first is usually endowed with prevalence by our courts, after

assess and weigh all the elements at stake.

However, preponderance does not mean prevalence when, after all the

concurrent circumstances in a specific case, the limits set are exceeded

normatively and jurisprudentially.

In this sense, the Article 29 Working Group in its Opinion 06/2014 on the

concept of legitimate interest of the data controller under the

Article 7 of Directive 95/46/EC, when examining the legal basis of the legitimate interest of the

Article 7.1.f) of Directive 95/46/CE, fully transferable to the current art. 6.1.f) of

GDPR, includes the right to freedom of expression or information as one of the

cases in which the question of legitimate interest may arise, stating that "without

regardless of whether the interests of the data controller will ultimately prevail

term on the interests and rights of the interested parties when the

weighing test".

V

Limits to the Fundamental Right to Freedom of Information.

That said, the Fundamental Right to Freedom of Information is not

absolute. We can observe very clear limits established by the courts in the

civil sphere, in relation to the Right to Honor, to Personal and Family Privacy and to

the Image itself.

Thus, we will cite, for all, the STC 27/2020, of February 24, 2020 (appeal of

amparo 1369-2017) that provides, in relation to the image of a person, and

starting from the incontrovertible fact that makes it identifiable, that "...the question
discussed is reduced to pondering whether the non-consented reproduction of the image of a
anonymous person, that is, someone who is not a public figure, but who acquires
suddenly and involuntarily a role in the newsworthy event, in this case as
victim of the failed attempted murder by his brother and the subsequent suicide
of this, supposed an illegitimate interference in his fundamental right to his own
image (art. 18.1 CE).

[…]

…that criminal events are newsworthy events, even with
regardless of the character of private subject of the person affected by the news. Without
However, the limit is in the individualization, direct or indirect, of the victim, since
This data is not of public interest because it lacks relevance for the information
that is allowed to be transmitted (SSTC 20/1992, of February 20; 219/1992, of
December; 232/1993, of July 12; 52/2002, of February 25; 121/2002, of 20
May, and 127/2003, of June 30). Thus, it is currently recognized by Law 4/2015, of 27
April, of the crime victim statute, in force since October 28, 2015,
when he warns of the need "from the public authorities [to offer] a
response as broad as possible, not only legal but also social, to the victims,
not only repairing the damage in the framework of a criminal proceeding, but also
minimizing other traumatic effects on the moral that his condition can
generate, all this regardless of their procedural situation. Therefore, the present
Statute, in line with European regulations on the matter and with the demands that
raises our society, claims, based on the recognition of the dignity of
victims, the defense of their material and moral assets and, with it, those of the group of

the society". In cases such as those raised in this appeal, this Court must

give relevance to the prevalence of the right to the image of the victim of the crime

against information freedoms, since graphic information became idle or

superfluous because the photograph of the victim lacks real interest for the transmission of

the information, in this case the apparent accomplishment of a homicide and subsequent

suicide" (emphasis added).

We will add the STS, from its First Civil Chamber, 272/2011 of April 11, 2011

(rec. 1747/2008), in which, regarding the data necessary to provide a

information and limits to the public interest states that "b) Trivial information is not

protects (ATC 75/2006), but the fact of providing unnecessary data in a case of

rape (full name, last name initials, street portal where

the victim lived) that have no community relevance, do not respect the reservation, only

seek to satisfy curiosity, produce disturbances or annoyances, and reveal

aspects of personal and private life unnecessarily, allowing neighbors,

close people and relatives full identification of the victim and knowledge

in great detail about an act that seriously violated his dignity (STC

185/2002) or about a disease that has no public interest and affects

direct to the irreducible field of intimacy and that reveals itself to the effect of a pure

joke or joke (STC 232/1993);".

Likewise, the STS, of its First Civil Chamber, Judgment 661/2016 of 10

November 2016 (rec. 3318/2014), in relation to the recruitment and disclosure in court

of the image of a victim of gender violence provided that "1.) The

interest of the questioned information nor the right of the defendant television channel

to broadcast images recorded during the act of the oral trial of the criminal case, since they did not

There is no limitation in this regard agreed by the judicial body.

2nd) The only controversial point is, therefore, whether the applicant's identification

as a victim of the crimes prosecuted in said criminal case, through first

shots of his face and the mention of his first name and place of residence, he was

also included in the fundamental right of the television channel

demanded to transmit truthful information or, on the contrary, was limited by the

fundamental rights of the plaintiff to her personal privacy and to her own

image.

3rd) Regarding this matter, the jurisprudence has recognized the general interest and the

public relevance of information on criminal cases (judgment 547/2011, of 20

July), which are accentuated in cases of physical and psychological abuse (judgments

128/2011, of March 1, and 547/2011, of July 20), but it has also pointed out,

regarding the identification of the persons involved in the trial, that the

defendant and the victim are not on an equal footing, because in terms of

that one does allow a complete identification, and not only by its initials, due to the

nature and social significance of the crimes of mistreatment (judgment 547/2011,

of July 20).

[…]

6th) In short, the defendant television channel should have acted with the prudence of the

diligent professional and avoid issuing images that represented the

recurring in close-up, either refraining from issuing the corresponding shots,

well using technical procedures to blur their features and prevent their

recognition (judgment 311/2013, of May 8). Similarly, it should also

avoid mentioning your first name, because this information, insufficient by itself to

constitute illegitimate interference, became relevant when pronounced on the screen

simultaneously with the image of the applicant and add the mention of her

town of residence, data all of them unnecessary for the essence of the content

information, as evidenced by the news about the same trial published in the

next day in other media. 7th) The identification of the plaintiff through his

image and personal data indicated and its direct link to an episode of

gender violence and other serious crimes, when disclosure was foreseeable

Simultaneous or subsequent data referring to how the victim and her aggressor met

and the way in which the criminal acts occurred, supposes that the loss of the

anonymity would violate both the plaintiff's right to her own image, by the

broadcast of their physical features, such as their personal and family intimacy, to the extent that

that some reserved data, belonging to his private life (who went to the Internet

to start a relationship or the intimate content of some of their talks), lacking

offensive entity in a situation of anonymity, they began to have it from the moment

in which any person who watched those news programs and who resided in the

location of the victim could know who they were referring to, so that the damage

psychological damage inherent to his condition as a victim of crimes was added to the moral damage

consisting of the disclosure of information about his private life that he had not consented to

make public." (underlining is ours).

As we can see, a clear reference is made to the excessive treatment of

personal data (some of which are not of an intimate nature) to provide the

information, considering them unnecessary at all points in attention to the

concurrent circumstances. Sometimes the courts refer to intimate data,

but sometimes it is personal data that is not intimate, such as, for

For example, the image of a natural person obtained from a photograph published in a

social network or name and surname.

SAW

Balance between the Fundamental Right to Freedom of Information and the Right

Fundamental to the Protection of Personal Data.

In the specific case examined, as we have indicated, the claimed party

published, on the website referred to in the facts, the audio of the statement before the judge

of a victim of a multiple rape, to illustrate the news of a very

media.

Thus, it is not a question, as in other cases examined by jurisprudence, of endowing

of prevalence to a fundamental right over another, having to choose which one has more

weight in a specific case. If not, rather, to find a balance between

both to achieve the achievement of the purpose of the first without undermining the second.

The reconciliation of both rights is nothing new, since the legislator

European Union mandates such reconciliation in article 85 of the GDPR.

As we have seen previously, the Fundamental Right to Freedom of

Information is not unlimited, since the jurisprudential interpretation when confronting it

with other rights and freedoms does not allow the same in any case and with all breadth,

but, nevertheless, the prevalence that the courts usually endow it can be seen

limited by other fundamental rights that must also be respected. Thus

observes its limitation when the personal data provided was unnecessary for the

essence of the information content.

We must consider the special circumstances present in the supposed

examined. It is about a very young woman who has suffered a multiple rape. In

In the published recording, she is heard recounting, with great emotional charge, the

sexual assault suffered in all crudeness, narrating (...).

In addition, we cannot lose sight of the victim status of the woman whose voice, with

all the nuances exposed, has spread.

Let us remember, for merely illustrative purposes, that Law 4/2015, of April 27,

of the Statute of the victim of the crime foresees a special need of protection to the

victims of crimes against sexual freedom or sexual indemnity, as well as

victims of violent crimes, both circumstances that concur in the alleged

examined.

In this case, the situation of the victim must be considered (who is not in the

same level of equality as the defendants) and what the diffusion of their voice with

all its nuances, as well as the special protection that the

legal system that, without constraining the supply of information, must be done

compatible with the principle of data minimization, applicable to the form, the

medium in which the information is supplied and disseminated due to the immediate affectation of the data

personnel and the identification of the victim.

Precisely because the obvious informative public interest in the news is not denied,

Given the general interest in criminal cases, in this specific case, it is not a question of

to diminish the Fundamental Right to Freedom of Information due to the prevalence

of the Fundamental Right to the Protection of Personal Data, but of

make them fully compatible so that both are absolutely

guaranteed. That is, the freedom of information of the media is not questioned.

of communication but the weighting with the right to data protection based on

to the proportionality and need to publish the specific personal data of the voice. Such

situation could have been resolved with the use of technical procedures to

prevent voice recognition, such as, for example, distortion of the voice of

the victim or the transcript of the report of the multiple rape, security measures

both, applied depending on the case in an ordinary way by means of

communication.

At older we have to mean that the victim is an anonymous person and our

Constitutional Court, for all STC 58/2018 of June 4, affirms that the

public authorities, public officials and public figures or those dedicated to

activities that carry public notoriety “voluntarily accept the risk of

that their subjective personality rights are affected by criticism, opinions

or adverse disclosures and, therefore, the right to information reaches, in relation to

with them, its maximum level of legitimizing effectiveness, insofar as their life and conduct

morality participate in the general interest with a greater intensity than that of those

private persons who, without a vocation for public projection, see themselves

circumstantially involved in matters of public importance, to which

Therefore, a higher level of privacy must be recognized, which prevents

granting general importance to facts or behaviors that would have it if they were referred to

to public figures".

The STJUE (Second Chamber) of February 14, 2019, in case C 345/17, Sergejs

Buivids mentions various criteria to ponder between the right to respect for

privacy and the right to freedom of expression, among which are “the

contribution to a debate of general interest, the notoriety of the affected person, the

object of the report, the previous behavior of the interested party, the content, the form and

the repercussions of the publication, the way and the circumstances in which it was obtained

information and its veracity (see, in this regard, the judgment of the ECtHR of 27

June 2017, Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland,

CE:ECHR:2017:0627JUD000093113, section 165)".

In such a way that for a matter to be considered of general interest,

public relevance, they will be not only for the person who intervenes, but also for the

matter to which it refers. Both requirements must concur, resulting, at greater

abundance of what was meant in the previous section, that in the case examined

the victim is not a public person; rather the contrary, it is of great interest that

is recognized by third parties, so it may entail a new penalty

to the already suffered The victim is an anonymous person and must remain so, in such a way that

so that their fundamental rights are fully guaranteed.

In the present case, (i) we are not dealing with a figure of public relevance, in which

sense that such relevance is sufficient to understand that it supposes, ex lege, a

dispossession of your fundamental right to the protection of your personal data, and (ii)

although we are dealing with facts "of public relevance", in the sense that they are revealed

as "necessary" for the presentation of ideas or opinions of public interest, that

necessity does not reach the provision of data that identifies the victim.

For this reason, and as expressed by the Supreme Court in its (civil) judgment 697/2019, of 19

December 2019, the formation of a free public opinion does not require, nor justify,
that the fundamental right to one's own image is affected [in this case to the protection
of personal data] with that seriousness and in a way that does not save the necessary
connection with the identification of the person object of the information.
It is worth mentioning the breach of point 1 of the Digital Pact for the
protection of persons, signed by the entities involved, which establishes that
"The signatories of the Charter will refrain from identifying the victims in any way.
of assaults, acts of violence or sexual content in their information or
publish information from which, in general, your identity can be inferred
in the case of people of no public relevance. All this without prejudice to the fact that the
non-public persons may be involved in newsworthy events, in which case
the informative coverage will be the necessary one to give adequate fulfillment to the right
information, taking into account the peculiarities of each case".
VII
Every person responsible for the treatment has conferred obligations in terms of
data protection, in the terms prescribed in the GDPR and in the LOPDGDD,
being able to highlight, in terms of what interests us, proactive responsibility,
Article 5.2 of the GDPR, risk assessment and implementation of measures
of adequate security. Obligations that are even more relevant when, as in
In the case we are examining, this one is especially sensitive.
Such obligations do not decline because we are before a data controller
that it is a means of communication.
If we add the diffusion of the victim's voice (with all its nuances), which makes it
identifiable and can be recognized by third parties, with the factual account that makes
in relation to the violation suffered, there is a very high and very likely risk that
may suffer damage to their rights and freedoms. This has happened in other cases

of dissemination of personal data of victims of rape crimes. And this, in addition to

that with the diffusion of the voice of the victim she is being sentenced again to

can be recognized by third parties, when it is not a proportional treatment or

necessary in relation to the information purposes pursued.

VIII

Excess data processing

In the present case, the defendant party has not presented allegations or evidence that

contradict the facts denounced within the period given for it.

In accordance with the evidence that is available and that has not been

distorted during the disciplinary procedure, it is considered that the party

claimed has processed data that was excessive as it was not necessary for the purpose

for which they were treated.

In view of the foregoing, the facts imply a violation of what is established in the

Article 5.1 c) of the GDPR, which implies the commission of an offense classified in the

Article 83.5, section a) of the GDPR, which under the heading "General conditions for

the imposition of administrative fines" provides that:

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:

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

consent in accordance with articles 5, 6, 7 and 9;”

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

offenses 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. Offenses considered very serious.

"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.”

IX

Classification of the offense

In the present case, based on the facts exposed, it is considered that the sanction

that corresponds to impose is an administrative fine. In order to determine the fine

the provisions of articles 83.1 and 83.2 of the GDPR must be observed, precepts

which point out:

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

under this Article for infringements of this Regulation

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

proportionate and dissuasive."

"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

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 controller or processor to

alleviate the damages and losses suffered by the interested parties;

d) the degree of responsibility of the controller or processor,

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 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 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 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."

Regarding section k) of article 83.2 of the GDPR, the LOPDGDD, article 76,

"Sanctions and corrective measures", provides:

"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."

Taking into account the precepts transcribed, for the purpose of setting the amount of the sanction of

fine to be imposed in the present case for the offense classified in article 83.5 a)

of the GDPR, it is appropriate to graduate it according to the following aggravating circumstances:

- Article 83.2.a) of the GDPR:

Nature, seriousness and duration of the infringement: The Agency considers that the

nature of the offense is very serious since it entails a loss of

provision and control over personal data to a person who has been a victim of

a violent crime and against sexual integrity and that by disseminating your personal data

condemns her again to be recognized by third parties, causing serious damage and

damages.

- Article 83.2.b) of the GDPR.

Intentional or negligent infringement: Although the Agency considers that it is not

there was intentionality on the part of the communication medium, the Agency concludes that

was negligent in not ensuring a procedure that guaranteed the protection of the

personal data in such sensitive circumstances, especially when in many

Sometimes the voice in the news is distorted so that it is not recognized

to the person speaking.

- Article 83.2.g) of the GDPR.

Categories of personal data affected by the infringement: The certain possibility of

recognize the victim of a crime as the one reporting the news, very serious, violent

and against sexual integrity (multiple rape), is seriously detrimental to the

affected, since what happened is linked to their sexual life.

The balance of the circumstances contemplated, with respect to the infraction committed

by violating the provisions of article 5.1 c) of the GDPR, it allows setting a fine of 50,000

€ (fifty thousand euros).

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 DISPLAY CONNECTORS, S.L., with NIF B65749715, for a

infringement of Article 5.1.c) of the GDPR, typified in Article 83.5 a) of the GDPR, a

fine of €50,000 (fifty thousand euros).

SECOND: NOTIFY this resolution to DISPLAY CONNECTORS, 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 number ES00 0000 0000 0000 0000 0000, open in the name of the Agency

Spanish Data Protection Agency at the bank CAIXABANK, S.A.. In the event

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

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-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

938-050522

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es