 File No.: EXP202102433

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. and D.B.B.B. (hereinafter the claiming party) dated

08/09/2021 filed a claim with the Spanish Data Protection Agency.

The claim is directed against D.C.C.C. with NIF ***NIF.1 (hereinafter the claimed).

The reasons on which the claim is based are the following: the claimants

They state that they received on 08/07/2021 messages from the address

***EMAIL.1 and the claimant in which the recipients do not appear "in blind carbon copies".

They provide:

- Screenshot of the email inbox in which

there are two emails from the defendant. For both the column

shows the subject “HORROR DINNER HORROR DINNER a

unforgettable experience starring a picturesque fam…”.

- Screenshot of the opening of an email subject "HORROR

DINNER” and date 08/07/2021 (3:37 hours); the content of the message is not observed

but it does partially list a plurality of recipients (email addresses

email) to whom the email would have been sent. As they state "in

The addresses don't end all over the screen, if I continue going down there would be even more

addresses, since there are a total of more than 190, as Hotmail tells me when

I open the email.”

- Screenshot of the opening of an email subject "HORROR

DINNER” and date 08/07/2021 (3:40 hours). The content is not observed in the capture

of the message but partially the list of a plurality of recipients

(email addresses) to whom the email would have been sent.

As they state "as before, in a single screenshot you do not see all the

addresses, if we continue going down, many more appear, until we reach almost 200”.

- Screenshot of opening a subject email “Re: HORROR

DINNER" and dated 08/07/2021 (8:21 a.m.) addressed to the claimant. The message warns

that you have not authorized to provide your data to other people and request that they remove you from

the mailing list to which you would have been placed without your permission.

- Screenshot of opening a subject email “Re: HORROR

DINNER”

reclaimed

info@screamentertainment.es. The content of the message coincides with that mentioned in the

previous paragraph.

- Screenshot of the opening of an email subject “Ezin da bidali:

Re: HORROR DINNER” and dated 08/07/2021 (11:47 am) directed by “Microsoft

Outlook <postmaster@outlook.com>” in which (in Basque language) you are informed

that the email described in the previous point could not be delivered to

the address info@screamentertainment.es.

- Screenshot of the opening of an email subject "HORROR

DINNER” and date 08/07/2021 (5:42 hours). In the capture the content of the and the list of

dated 08/07/2021 (11:46 a.m.) addressed to

and

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

a plurality of recipients (email addresses) to which the

sent the email. The message advertises an event organized by the

claimed and refers the website ***URL.1.

- Screenshot of the opening of an email dated 07/08/2021

(6:42 hours) addressed to the defendant in which he requests the removal of his data from the

database.

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), on 10/01/2021 the claim was transferred to the

claimed, in accordance with the LPACAP, to proceed to its analysis and

inform this Agency within a month of the actions carried out to

adapt to the requirements set forth in the data protection regulations. Not included or provided

respondent's response.

THIRD: On 11/17/2021, in accordance with article 65 of the LOPDGDD,

The claim presented by the complaining 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 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:

On 11/24/2021, the requested request was addressed to him requesting him to facilitate the

following information in relation to the facts investigated:

"1.- Reason for which the email attached to this request was sent without

blind copy, that is, showing the addresses of the rest of the recipients to all

they.

2.- Description of the procedure established for the submission of this type of

communications. Copy of the instructions addressed to the personnel in charge of its

shipment.

3.- Actions taken in order to minimize the adverse effects of this incident and

those adopted for their final resolution indicating the dates on which they have been executed.

4.- If applicable, reason why the security breach has not been notified to this

Agency.

5.- If applicable, information on the notification of the security breach to the

affected, indicating the means of referral and providing a copy of the notification sent.

6.- If applicable, information on whether other mailings have been produced

similar without blind copying of the recipients.

7.- Technical and organizational measures adopted to avoid, as far as possible, incidents

security as the one that happened."

The requirement was delivered on 12/07/2021. expiration of the term

granted, there is no answer in the information systems of the AEPD.

The request for information was addressed to the claimant at the postal address

***ADDRESS 1.

There is Diligence of the acting inspector with information collected from the internet in

relation to the defendant:

- The legal notice incorporated into the website ***URL.1 (referred to in the emails

object of claim) cites the following regarding the person responsible:

“Data about the person responsible for this website and the domain www.screamfarmgroup.com.

Company name is: Scream Farm Group CIF: ***NIF.1 Its registered office is in

Celler 6, Penthouse B, 07141 Marratxi, Palma de Mallorca.

[…] Email: info@screamentertainment.es

[…] Legitimation for data processing: The legal basis for the processing of your

data of the above purposes is the execution of the provision of the service

correspondent. The prospective offer of products and services to customers and users

is based on the satisfaction of the legitimate business interest consisting of being able to

offer our clients the contracting of other products or services and obtain

So your loyalty. Said legitimate interest is recognized by the applicable legal regulations

(General Data Protection Regulation), which expressly allows the

processing of personal data on that legal basis for marketing purposes

direct. However, we remind you that you have the right to oppose this treatment

of your data, being able to do so by any of the means described in this Policy.

The basis for sending commercial communications to non-customer users is the

consent that has been requested, and may be revoked at any time. The

Withdrawal of said consent will not affect in any case the execution of the

contract, but data processing for this purpose carried out previously does not

they will lose their legality due to the fact that the consent has been revoked.

[…] Contact In the event that any User has any questions about these

Legal conditions or any comments about our website, please go to

***EMAIL.2 or through the contact section.”

- The legal notice incorporated into the website ***URL.2/ that refers to information

analogous to that provided in the previous paragraph.

FIFTH: On 04/29/2022, the Director of the Spanish Agency for the Protection of

Datos agreed to initiate disciplinary proceedings against the defendant, for the alleged

violation of articles 32.1 and 5.1.f) of the GDPR, typified in article 83.4.a) and

83.5.a) of the GDPR, with warning. Receipt by the claimant of the

agreement to start the file.

SIXTH: Notified of the initiation agreement, the claimant at the time of this

resolution has not submitted a written statement of allegations, so the following applies

indicated in article 64 of Law 39/2015, of October 1, on the Procedure

Common Administrative Law of Public Administrations, which in its section f)

establishes that in the event of not making allegations within the period established on the

content of the initiation agreement, it may be considered a proposal for

resolution when it contains a precise pronouncement about the responsibility

accused, for which reason a Resolution is issued.

SEVENTH: Of the actions carried out in this procedure, have been

the following accredited:

PROVEN FACTS

FIRST: On 08/09/2021 there is a written entry in the AEPD from the complaining party

stating that they have received emails on 08/07/2021

from the address ***EMAIL.1 and from the defendant in which the recipients do not

They are "blind copies".

SECOND: The complaining party has provided screenshots of the mailbox

e-mail entry containing e-mails from the

reclaimed

THIRD: The following information provided by the State Agency for

Tax Administration (AEAT), in relation to the data associated with NIF ***NIF.1

"C.C.C." with tax domicile in

that appear in their databases:

"***ADDRESS 1"

FOURTH: Proceedings of the acting inspector containing information

obtained from the internet related to the claimed:

- The legal notice incorporated into the ***URL.1 internet site, citing the following insofar as

to your manager:

“Data about the person responsible for this website and the domain www.screamfarmgroup.com.

Company name is: Scream Farm Group CIF: ***NIF.1 Its registered office is in

Celler 6, Penthouse B, 07141 Marratxi, Palma de Mallorca.

[…] Email: info@screamentertainment.es

[…] Legitimation for data processing: The legal basis for the processing of your

data of the above purposes is the execution of the provision of the service

correspondent. The prospective offer of products and services to customers and users

is based on the satisfaction of the legitimate business interest consisting of being able to

offer our clients the contracting of other products or services and obtain

So your loyalty. Said legitimate interest is recognized by the applicable legal regulations

(General Data Protection Regulation), which expressly allows the

processing of personal data on that legal basis for marketing purposes

direct. However, we remind you that you have the right to oppose this treatment

of your data, being able to do so by any of the means described in this Policy.

The basis for sending commercial communications to non-customer users is the

consent that has been requested, and may be revoked at any time. The

Withdrawal of said consent will not affect in any case the execution of the

contract, but data processing for this purpose carried out previously does not

they will lose their legality due to the fact that the consent has been revoked.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/12

[…] Contact In the event that any User has any questions about these

Legal conditions or any comments about our website, please go to

***EMAIL.2 or through the contact section."

- The legal notice incorporated into the website ***URL.2 containing information

analogous to that provided in the previous paragraph.

FUNDAMENTALS OF LAW

Yo

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter GDPR), grants each

control authority and as established in articles 47, 48.1, 64.2 and 68.1 of the

Organic Law 3/2018, of December 5, on the Protection of Personal Data and

guarantee of digital rights (hereinafter, LOPDGDD), is competent to

initiate and resolve this procedure the Director of the Spanish Protection Agency

of data.

Likewise, article 63.2 of the LOPDGDD determines that: "The

procedures processed by the Spanish Data Protection Agency will be governed

by the provisions of Regulation (EU) 2016/679, in this organic law, for the

regulatory provisions dictated in its development and, as soon as they are not

contradict, on a subsidiary basis, by the general rules on the

administrative procedures."

The facts claimed materialize in the receipt of emails

from the address ***EMAIL.1 belonging to the defendant in which the

recipients are not "blind carbon copies".

II

Article 5 of the GDPR establishes the principles that must govern the treatment

of personal data and mentions among them that of "integrity and confidentiality".

The cited article states that:

"1. Personal data will be:

(…)

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

personal data, including protection against unauthorized processing or

illicit and against its loss, destruction or accidental damage, through the application

of appropriate technical or organizational measures ("integrity and

confidentiality").

(…)

The documentation in the file offers clear indications that the

claimed, violated article 5 of the RGPD, principles related to treatment, by sending

email without using the blind copy option violating confidentiality

in the processing of personal data. Thus, the claimant had

access to the email addresses of other recipients.

This duty of confidentiality must be understood as its purpose

prevent access to the data without the consent of the owners of the data

themselves.

Therefore, this duty of confidentiality is an obligation that incumbents not

only to the person in charge and in charge of the treatment but to everyone who intervenes in

any phase of the treatment and complementary to the duty of professional secrecy.

IV.

Article 83.5 a) of the GDPR, considers that the infringement of "the principles

principles for treatment, including the conditions for consent under

of articles 5, 6, 7 and 9" is punishable, in accordance with section 5 of the

mentioned Article 83 of the aforementioned Regulation, "with administrative fines of

€20,000,000 maximum or, in the case of a company, an equivalent amount

at a maximum of 4% of the overall annual total turnover of the financial year

above, opting for the one with the highest amount".

The LOPDGDD in its article 71, Violations, states 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".

And in its article 72, it considers for the purposes of prescription, which are: "Infractions

considered very serious:

1. Based on what is established in article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

suppose a substantial violation of the articles mentioned in that 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.

(…)

Secondly, article 32 of the GDPR "Security of treatment",

V

states that:

"1. Taking into account the state of the art, the application costs, and the

nature, scope, context and purposes of processing, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical and

appropriate organizational measures to guarantee a level of security appropriate to the risk,

which may include, among others:

a) the pseudonymization and encryption of personal data;

b) the ability to ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and assessment of effectiveness

technical and organizational measures to guarantee the safety of the

treatment.

2. When evaluating the adequacy of the level of security, particular attention should be paid to
take into account the risks presented by data processing, in particular as
consequence of the destruction, loss or accidental or illegal alteration of data
personal information transmitted, preserved or processed in another way, or the communication or
unauthorized access to such data.
3. Adherence to an approved code of conduct pursuant to article 40 or to a
certification mechanism approved under article 42 may serve as an element
to demonstrate compliance with the requirements established in section 1 of the
present article.
4. The person in charge and the person in charge of the treatment will take measures to
ensure that any person acting under the authority of the controller or the
manager and has access to personal data can only process such data
following the instructions of the person in charge, unless it is obliged to do so by virtue of the
Law of the Union or of the Member States".
The violation of article 32 of the GDPR is typified in article
83.4.a) of the aforementioned GDPR in the following terms:
SAW
"4. Violations of the following provisions will be penalized, according to
with paragraph 2, with administrative fines of maximum EUR 10,000,000 or,
in the case of a company, an amount equivalent to a maximum of 2% of the
total annual global business volume of the previous financial year, opting for
the highest amount:
a) the obligations of the person in charge and the person in charge according to articles 8,
11, 25 to 39, 42 and 43.
(…)"
For its part, the LOPDGDD in its article 73, for prescription purposes, qualifies

of "Infringements considered serious":

"Based on what is established in article 83.4 of Regulation (EU) 2016/679

are considered serious and will prescribe after two years the infractions that suppose a

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

following:

(…)

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

are appropriate to guarantee a level of security appropriate to the risk

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

8/12

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

(EU) 2016/679.

(…)"

The GDPR defines breaches of personal data security as

"all those security violations that cause the destruction, loss or

accidental or illegal alteration of personal data transmitted, stored or processed

otherwise, or unauthorized disclosure of or access to such data."

VII

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

that the defendant has violated article 32 of the GDPR, when an incident of

security when sending email to a large number of recipients without the

blind carbon copy function, without having adequate technical and organizational measures.

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

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

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

treatment will apply technical and organizational measures that are appropriate to the risk

that entails the treatment, taking into account the state of the art, the costs of

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

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

In addition, security measures must be adequate and

proportionate to the risk detected, noting that the determination of the measures

technical and organizational procedures must be carried out taking into account: pseudonymization and

encryption, the ability to ensure confidentiality, integrity, availability and

resiliency, the ability to restore availability and access to data after a

incident, verification process (not audit), evaluation and assessment of the

effectiveness of the measures.

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

particular account of the risks presented by data processing, such as

consequence of the destruction, loss or accidental or illegal alteration of data

personal information transmitted, preserved or processed in another way, or the communication or

unauthorized access to said data and that could cause damages

physical, material or immaterial.

In this sense, recital 83 of the GDPR states that:

"(83) In order to maintain security and prevent processing from infringing what

provided in this Regulation, the person in charge or in charge must evaluate

the risks inherent to the treatment and apply measures to mitigate them, such as the

encryption. These measures must ensure an adequate level of security, including the

confidentiality, taking into account the state of the art and the cost of its application

regarding the risks and nature of the personal data to be

protect yourself. When assessing risk in relation to data security, considerations should be

take into account the risks arising from the processing of personal data,

such as the destruction, loss or accidental or unlawful alteration of personal data

transmitted, stored or processed in another way, or communication or access not

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

The responsibility of the defendant is determined by the incident of

security evidenced by the claimant, since he is responsible for taking

decisions aimed at effectively implementing the technical and

appropriate organizational measures to guarantee a level of security appropriate to the risk

to ensure the confidentiality of the data, restoring its availability and preventing

access to them in the event of a physical or technical incident. However, from the

documentation provided shows that the entity has not only breached this

obligation, but also the adoption of measures in this regard is unknown,

despite having notified him of the claim presented.

Pursuant to the foregoing, it is estimated that the defendant would be

allegedly responsible for the infringement of article 32 of the GDPR, infringement

typified in its article 83.4.a).

In order to establish the administrative fine that should be imposed, the

observe the provisions contained in articles 83.1 and 83.2 of the GDPR, which

point out:

VIII

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

administrative proceedings under this article for violations of this

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

effective, proportionate and dissuasive.

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

of each individual case, as an addition to or substitute for 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 the number of stakeholders affected and the level of damage and

damages they have suffered;

b) intentionality or negligence in the infringement;

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 the person in charge of the

processing, taking into account the technical or organizational measures that have

applied under articles 25 and 32;

e) any previous infringement committed by the person in charge or in charge of the

treatment;

f) the degree of cooperation with the supervisory authority in order to put

remedy the breach and mitigate the potential adverse effects of the breach;

g) the categories of personal data affected by the infringement;

h) the way in which the supervisory authority became aware of the infringement, in

particularly if the person in charge or the person in charge notified the infringement and, in such a case,

what extent;

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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

previously ordered against the person in charge or in charge in question

in relation to the same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or to 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 the financial benefits obtained or the losses avoided, direct

or indirectly, through the infringement.

In relation to letter k) of article 83.2 of the GDPR, the LOPDGDD, in its

Article 76, "Sanctions and corrective measures", establishes that:

"2. In accordance with the provisions of article 83.2.k) of the Regulation (EU)

2016/679 may also be taken into account:

a) The continuing nature of the offence.

b) Linking the activity of the offender with the performance of processing

of personal data.

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

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

commission of the offence.

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

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

f) The affectation of the rights of minors.

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

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

voluntary, alternative conflict resolution mechanisms, in those

cases in which there are controversies between those and any

interested."

data.

- In accordance with the precepts transcribed, for the purpose of setting the amount of the

sanction of a fine to be imposed in the present case for the offense typified in the

Article 83.5.a) and Article 5.1.f) of the GDPR for which the defendant is held responsible, in

In an initial assessment, the following factors are considered concurrent:

They are aggravating circumstances:

The linking of the activity of the offender with the performance of treatment of

Personal data.

In accordance with the above factors, it is deemed appropriate to impose on the defendant

for violation of article 5.1.f) of the GDPR, a penalty of 3,000 euros.

- Secondly, for the purposes of setting the amount of the fine to

impose in the present case for the infringement typified in article 83.4.a) and article

32.1 of the GDPR for which the defendant is held responsible, in an initial assessment,

considers it appropriate to impose a penalty of 2,000 euros on the defendant.

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 D.C.C.C., with NIF ***NIF.1, for a violation of article

5.1.f) of the GDPR, typified in article 83.5, a) of the GDPR, a fine of €3,000 (three

a thousand euros).

SECOND: IMPOSE D.C.C.C., with NIF ***NIF.1, for a violation of article

32.1 of the GDPR, typified in article 83.4, a) of the GDPR, a fine of €2,000 (two

a thousand euros).

THIRD: NOTIFY this resolution to D.C.C.C..

FOURTH: Warn the sanctioned party that he must enforce the sanction imposed

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 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, 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

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es