 File No.: EXP202105669

RESOLUTION OF SANCTIONING PROCEDURE

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

BACKGROUND

FIRST: D.A.A.A. (hereinafter, the claiming party), on November 8,
2021, filed a claim with the Spanish Agency for Data Protection. The
The claim is directed against the DEPARTMENT OF EDUCATION, CULTURE AND
DEPORTE, with NIF S5011001D, (hereinafter, the claimed party). The reasons in
on which the claim is based are as follows:

The claimant states that the General Directorate of Personnel Management of the
department in which it provides services (Education, Culture and Sport) sent, in
dated September 28, 2021, an email attaching a
Excel sheet with the data of more than 200 employees disclosing to third parties their
names and surnames, ID, job position and an additional cell to indicate if
wished to carry out a medical examination, without the express consent of the
owners of said data.

On September 30, 2021, the claimant sent an email to the
Data Protection Unit of the Government of Aragon reporting the incident.

On October 19, 2021, said Data Protection Unit put into
knowledge of the claimant that said department had been informed of the
need to carry out technical and organizational measures that prevent the access of
third parties to personal data, both identifying and special category.

Along with the claim, it provides an email sent on September 28,
2021, the Excel sheet in which you can view personal data from more than 200

employees (including those of the claimant himself) and the email communicating

incident and response.

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

December, Protection of Personal Data and Guarantee of Digital Rights

(hereinafter LOPDGDD), said claim was transferred to the claimed party,

to proceed with its analysis and inform this Agency within a month,

of the actions carried out to adapt to the requirements established in the

data protection regulations.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

Public (hereinafter, LPACAP) by electronic notification, was not collected by

the person in charge, within the period of availability, understood as rejected

in accordance with the provisions of art. 43.2 of the LPACAP, dated January 3, 2022,

as stated in the certificate that is in the file.

Although the notification was validly made by electronic means, assuming that

carried out the procedure in accordance with the provisions of article 41.5 of the LPACAP, under

information, a copy was sent by postal mail, which was duly notified in

dated January 20, 2022. In said notification, he was reminded of his obligation to

interact electronically with the Administration, and were informed of the media

of access to said notifications, reiterating that, in the future, you will be notified

exclusively by electronic means.

No response has been received to this letter of transfer.

THIRD: On February 8, 2022, in accordance with article 65 of the

LOPDGDD, the admission for processing of the claim presented by the

complaining party.

FOURTH: On July 7, 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 articles 5.1.f) and 32 of the GDPR,

typified in articles 83.5 and 83.4 of the GDPR, respectively.

The initiation agreement was notified, in accordance with the regulations established in the Law

39/2015, of October 1, of the Common Administrative Procedure of the

Public Administrations (hereinafter, LPACAP), on July 26, 2022, as

It is stated in the certificate that is in the file.

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

Law 39/2015, of October 1, on the Common Administrative Procedure of

Public Administrations (hereinafter, LPACAP), the claimed party submitted a written

of allegations in which, in summary, he stated that he requested a report from the

General Directorate of Personnel, this indicates that the referral was made to the accounts of

corporate mail of each organization, which are attended only by the

high-ranking secretaries in each of them, it is unknown if, for

For their part, the table was forwarded to the rest of the workers of each organization or if, as

seems more appropriate, it was the heads of each secretariat who consulted

personally to each partner about their preferences for carrying out the

medical examination.

Likewise, it states that the complainant did not receive in his email account

corporate staff of public employee the list, but had access to it through

of the corporate account of the General Management to which it is attached. This is the

General Directorate of Personnel did not disclose the data of the employees of the

department in mass mail addressed to all of them, but instead asked the people

held by the secretaries of the department's senior positions (the Directorates

General) that obtain the consent to the medical examination, assuming

fact that only people who have access to those tables would have access to that table.

corporate accounts and have it in the exercise of the functions that are theirs.

Finally, it adds that the General Directorate of Personnel will be required to promote

the review of the adequacy of the procedure that brings cause of the complaint to the

regulations in force on the matter (obtain the consent of public employees

to carry out the medical examination to which they are entitled), for which

will be sent to the Data Protection Delegate of this department, so that they

advise on this review and that the necessary measures be adopted, where appropriate,

in addition to those that are already implemented in this Administration.

SIXTH: On August 19, 2022, a resolution proposal was formulated,

proposing:

<< That by the Director of the Spanish Agency for Data Protection be imposed on the

DEPARTMENT OF EDUCATION, CULTURE AND SPORTS, with NIF S5011001D,

for a violation of article 5.1.f) of the GDPR, typified in article 83.5 of the GDPR,

a warning sanction and for a violation of article 32 of the GDPR, typified

in article 83.4 of the GDPR, a warning sanction.>>

The aforementioned resolution proposal was sent, in accordance with the rules established in Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations (hereinafter, LPACAP), by means of electronic notification, being received on August 22, 2022, as stated in the certificate that works on the record.

SEVENTH: The claimed party has not submitted allegations to the Proposal for Resolution.

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: It is on record that on November 8, 2021, the claimant filed a claim with the Spanish Agency for Data Protection, since the respondent party has disclosed personal information and data to third parties, without the express consent of the owners of said data.

SECOND: It is verified that it is an email in which a Excel sheet in which the data of more than 200 employees can be viewed by giving know third parties, their names and surnames, ID, job position and a cell additional information to indicate if they wished to undergo a medical examination.

THIRD: The claimed party states that it will proceed to review the adequacy of the procedure to the regulations in force on the matter.

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 Agency for Data Protection.

Likewise, article 63.2 of the LOPDGDD determines that: "The procedures processed by the Spanish Data Protection Agency will be governed by the provisions in Regulation (EU) 2016/679, in this organic law, by the provisions regulations dictated in its development and, insofar as they do not contradict them, with character subsidiary, by the general rules on administrative procedures."

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

II

In the first place, the documentation in the file proves that the party claimed, from the email address: ***EMAIL.1 sent an email email to the SGT and General Directorates, in which an Excel sheet was attached where you could see the name, surname, ID, job position of more than 200 public employees and an additional cell to indicate if they wished to carry out a medical examination.

The defendant has alleged that the referral was made to the email accounts corporate offices of each organization, which are attended solely by the secretaries of senior positions in each of them. However, what

occurs in this case does not conform to said scheme, since the information relative to the claimant is not only sent to his unit, but the complete list of all departments with the name, surname, ID, job position of more than 200 public employees, was within the reach of all recipient departments of said email. If some minimum security measures have been established in the sending the list, it could have been sent to each unit only the data of personnel attached to each of them. However, the complete list was sent to all. With this, even admitting the possibility that access to the corporate mailbox of each directorate general was restricted, the truth is that they were revealed to all units the personal data of personnel not attached to them. Also, the mail email in question, in turn, drags below, the one that DG Personnel received for the data collection was carried out. Well, neither one nor the other contain indications of precautions addressed to recipients so that the collection of data was collected with the utmost confidentiality, which points to a lack of measures of security.

In this sense, although email is a communication tool that facilitates and speeds up the operation of a company, despite its great benefits such as accessibility, speed and the possibility of attaching files, it is necessary to define a correct and safe use, since, in some Sometimes, employees can send confidential documents to those who do not They had to by mistake, or reveal personal data. In this sense it is very important make staff and users of corporate mail aware of threats and provide them with the appropriate tools to make safe use of it.

In the specific case under review, in relation to the category of data to which
third parties have had access, on the possibility of combining information
referring to a holder of personal data, the Opinion can be brought up
4/2007 of the Working Group of Article 29, "On the concept of personal data"
that analyzes the possibilities of identifying someone through combinations with
other information, starting only from the basic data and combining it with
other.

Specifically, it indicates the following: (...) when we speak of "indirectly"
identified or identifiable, we are referring in general to the phenomenon of
"unique combinations", be they small or large. In cases where, to
At first glance, the available identifiers do not make it possible to single out a person
given, it may still be "identifiable" because that combined information
with other data (whether the controller is aware of them
as if not) will allow distinguishing that person from others. This is where the Directive
refers to "one or several specific elements, characteristic of their physical identity,
physiological, psychological, economic, cultural or social. Some of those features
are so unique that they allow you to identify a person without effort (the "current
President of the Government of Spain"), but a combination of details
belonging to different categories (age, regional origin, etc.) can also be what
quite conclusive in some circumstances, especially if you have access to
additional information of a certain type. This phenomenon has been studied
widely by statisticians, always ready to avoid any
breach of confidentiality (…). So the different pieces come together.
that make up the personality of the individual in order to attribute certain

decisions. (…)

In this case, the Internet search, for example, of the name, surname of one of the

those affected can offer results that combining them with those now accessed

by third parties, allow us access to other applications of those affected or the

creation of personality profiles, which need not have been consented to by

its owner.

This possibility supposes an added risk that has to be assessed and that increases the

requirement of the degree of protection in relation to the safety and safeguarding of the

integrity and confidentiality of these data.

This risk must be taken into account by the data controller who, in

function of this, must establish the necessary technical and organizational measures that

prevents the data controller from losing control of the data and,

therefore, by the owners of the data that provided them.

Consequently, the allegations must be dismissed, meaning that the

arguments presented do not distort the essential content of the offense that

is declared committed nor does it imply sufficient justification or exculpation.

II

previous questions

The Department of Education, Culture and Sport of the Government of Aragon, like any other

any other public entity, is obliged to comply with Regulation (EU)

2016/679 of the European Parliament and of the Council of April 27, 2016, regarding the

protection of individuals with regard to the processing of personal data

and the free circulation of these data -RGPD-, and LO 3/2018, of December 5,

bre, Protection of Personal Data and Guarantee of Digital Rights -LO-

PDGDD- regarding the processing of personal data that they carry out,

understanding by personal data, "all information about a natural person

identified or identifiable.

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

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

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

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

economic, cultural or social of said person.

Likewise, treatment must be understood as “any operation or set of operations

tions made on personal data or sets of personal data, either by

automated procedures or not, such as the collection, registration, organization, structure

ration, conservation, adaptation or modification, extraction, consultation, use, co-

communication by transmission, diffusion or any other form of access authorization,

collation or interconnection, limitation, suppression or destruction”.

Taking into account the foregoing, the Department of Education, Culture and Sport pre-

ta a series of public services, for which it processes personal data of

its employees and citizens.

It carries out this activity in its capacity as data controller, since it is

who determines the purposes and means of such activity, by virtue of article 4.7 of the GDPR:

"responsible for the treatment" or "responsible": the natural or legal person, authority

public authority, service or other body that, alone or jointly with others, determines the purposes and

means of treatment; if the law of the Union or of the Member States determines

determines the purposes and means of the treatment, the person in charge of the treatment or the criteria

Specific reasons for their appointment may be established by the Law of the Union or of the

Member states.

Article 4 section 12 of the RGPD defines, in a broad way, the "violations of security"

security of personal data" (hereinafter security breach) as "all

those security violations that cause the destruction, loss or alteration

Accidental or illegal transfer of personal data transmitted, stored or processed in

otherwise, or unauthorized communication or access to such data."

In the present case, there is a personal data security breach in the

circumstances indicated above, categorized as a breach of confidentiality,

whenever the claimed party has disclosed information and data of a personal nature

to third parties, without the express consent of the owner of said data, by attaching to the

e-mail an Excel sheet containing the name, surname, ID, position of

work of more than 200 public employees and an additional cell to indicate if

They wanted to do the medical examination.

This type of data, as well as any other information that is referred to

individuals, are considered personal data, so their

Treatment is subject to data protection regulations.

According to GT29, a "Breach of confidentiality" occurs when there is

an unauthorized or accidental disclosure of personal data, or access to it

themselves.

It should be noted that the identification of a security breach does not imply the impossibility

sanction directly by this Agency, since it is necessary to analyze the

diligence of managers and managers and security measures applied.

Within the principles of treatment provided for in article 5 of the GDPR, the

integrity and confidentiality of personal data is guaranteed in section 1.f)

of article 5 of the GDPR. For its part, the security of personal data comes

regulated in article 32 of the GDPR, which regulates the security of the treatment.

IV.

Article 5.1.f) of the GDPR

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

"Article 5 Principles relating to treatment:

1. Personal data will be:

(…)

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

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

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

or organizational procedures (“integrity and confidentiality”).”

In relation to this principle, Recital 39 of the aforementioned GDPR states that:

“[…]Personal data must be processed in a way that guarantees security and

appropriate confidentiality of personal data, including to prevent access

or unauthorized use of said data and of the equipment used in the treatment”.

The documentation in the file offers clear indications that the

claimed violated article 5.1 f) of the GDPR, principles relating to treatment.

In the present case, according to documentation provided by the claimant and in the absence of

response of the claimed party, it can be verified that, from the direction of

email: ***EMAIL.1 An email has been sent containing the

attached an Excel sheet in which you can see the name, surname, ID,

workplace for more than 200 public employees and an additional cell for

indicate if they wished to undergo a medical examination.

The accredited facts constitute, on the part of the defendant, in his capacity as

responsible for the aforementioned processing of personal data, a violation of the

principle of confidentiality, by disseminating this information among employees without

certify that he had obtained their consent for that specific

treatment.

Consequently, it is considered that the accredited facts are constitutive of

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

GDPR.

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

V

The aforementioned infringement of article 5.1.f) of the GDPR supposes the commission of the infringements

typified in article 83.5 of the GDPR that under the heading "General conditions

for the imposition of administrative fines" provides:

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

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

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

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

the highest amount:

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

to)

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

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

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result

contrary to this organic law”.

For the purposes of the limitation period, article 72 "Infractions considered very

serious” of the LOPDGDD indicates:

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

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

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

following:

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

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

Article 32 of the GDPR, security of treatment, establishes the following:

SAW

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

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

variable probability and severity for the rights and freedoms of individuals

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

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

which may include, among others:

a) the pseudonymization and encryption of personal data;

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

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

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

technical and organizational measures to guarantee the safety of the

treatment.

2. When evaluating the adequacy of the security level, particular consideration will be given to

take into account the risks presented by data processing, in particular as

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

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

unauthorized access to such data.

3. Adherence to an approved code of conduct pursuant to article 40 or to a

certification mechanism approved under article 42 may serve as an element

to demonstrate compliance with the requirements established in section 1 of the

present article.

4. The controller and the processor shall take measures to ensure that

any person acting under the authority of the controller or processor and

have access to personal data can only process such data by following

instructions of the person in charge, unless it is obliged to do so by virtue of the Law of

the Union or of the Member States.

The facts revealed imply the lack of technical measures and

organizational by enabling the display of personal data of the claimant

with the consequent lack of diligence by the person in charge, allowing unauthorized access

authorized by third parties.

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 is the object of treatment, but it establishes that the person in charge and the person in charge of the treatment apply technical and organizational measures that are appropriate to the risk involved the treatment, taking into account the state of the art, the application costs, the nature, scope, context and purposes of processing, probability risks and seriousness for the rights and freedoms of the persons concerned.

In addition, security measures must be adequate and proportionate to the detected risk, noting that the determination of the technical measures and organizational procedures must be carried out taking into account: pseudonymization and encryption, the ability to ensure confidentiality, integrity, availability and resilience, the ability to restore availability and access to data after an incident, process verification (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 authorized to said data, susceptible in particular to cause damages physical, material or immaterial.

Recital 75 of the GDPR lists a series of factors or assumptions associated with risks to the guarantees of the rights and freedoms of the interested parties:

“The risks to the rights and freedoms of natural persons, serious and variable probability, may be due to data processing that could cause physical, material or immaterial damages and losses, particularly in cases in which that the treatment may give rise to problems of discrimination, usurpation of identity or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorized reversal of the pseudonymization or any other significant economic or social harm; in the cases in which the interested parties are deprived of their rights and freedoms or are prevent you from exercising control over your personal data; In cases where the data personal treaties reveal ethnic or racial origin, political opinions, religion or philosophical beliefs, union membership and genetic data processing,

data relating to health or data on sexual life, or convictions and offenses
criminal or related security measures; in cases where they are evaluated
personal aspects, in particular the analysis or prediction of aspects related to the
performance at work, economic situation, health, preferences or interests
personal, reliability or behavior, situation or movements, in order to create or
use personal profiles; in cases in which personal data of
vulnerable people, particularly children; or in cases where the treatment
involves a large amount of personal data and affects a large number of
interested."

In this sense, the Internet search, for example, of the name, surnames, ID or
email from one of those affected may offer results that
combining them with those now accessed by third parties, allow us access to other
applications of those affected or the creation of personality profiles, which do not have
why have been consented to by its owner.

The responsibility of the defendant is determined by the lack of measures of
security, since it is responsible for making decisions aimed at implementing
effectively the appropriate technical and organizational measures to guarantee a

level of security appropriate to the risk to ensure the confidentiality of the data,
restoring their availability and preventing access to them in the event of an incident
physical or technical Likewise, you must know the main risks to which you are
exposed corporate mail every time that privileged access to the environment of the

Mail is usually restricted to several people from the corresponding technical area, for

what the actions of said accesses must be conveniently traced to

detect any anomalous situation, especially those that may imply

confidentiality losses.

Therefore, the accredited facts constitute an infraction, attributable to the

claimed party, for violation of article 32 GDPR.

Classification of the infringement of article 32 of the GDPR

VII

The aforementioned infringement of article 32 of the GDPR supposes the commission of the infringements

typified in article 83.4 of the GDPR that under the heading "General conditions

for the imposition of administrative fines" provides:

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

paragraph 2, with administrative fines of maximum EUR 10,000,000 or,

in the case of a company, an amount equivalent to a maximum of 2% of the

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

the highest amount:

to)

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

11, 25 to 39, 42 and 43; (…)"

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

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result

contrary to this organic law".

For the purposes of the limitation period, article 73 "Infractions considered serious"

of the LOPDGDD indicates:

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

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

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

following:

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

are appropriate to ensure a level of security appropriate to the

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

Regulation (EU) 2016/679."

VIII

Responsibility

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Establishes Law 40/2015, of October 1, on the Legal Regime of the Public Sector, in

Chapter III relating to the "Principles of the Power to sanction", in article 28

under the heading "Responsibility", the following:

"1. They may only be penalized for acts constituting an administrative offense

physical and legal persons, as well as, when a Law recognizes their capacity to

act, the affected groups, the unions and entities without legal personality and the

independent or autonomous patrimonies, which are responsible for them

title of fraud or fault."

Lack of diligence in implementing appropriate security measures

with the consequence of the breach of the principle of confidentiality constitutes the

element of guilt.

IX

Sanction

Article 83 "General conditions for the imposition of administrative fines" of the

GDPR in its section 7 establishes:

"Without prejudice to the corrective powers of the control authorities under the

Article 58(2), each Member State may lay down rules on whether

can, and to what extent, impose administrative fines on authorities and bodies

public establishments established in that Member State."

Likewise, article 77 "Regime applicable to certain categories of

responsible or in charge of the treatment" of the LOPDGDD provides the following:

"1. The regime established in this article will be applicable to the treatment of

who are responsible or in charge:

(…)

c) The General State Administration, the Administrations of the communities

autonomous entities and the entities that make up the Local Administration.

2. When the managers or managers listed in section 1 commit

any of the offenses referred to in articles 72 to 74 of this law

organic, the data protection authority that is competent will dictate

resolution sanctioning them with a warning. The resolution will establish

likewise, the measures that should be adopted to cease the conduct or to correct it.

the effects of the offense committed.

The resolution will be notified to the person in charge or in charge of the treatment, to the body of the

that depends hierarchically, where appropriate, and to those affected who had the condition

interested, if any.

3. Without prejudice to what is established in the previous section, the data protection authority

data will also propose the initiation of disciplinary actions when there are

enough evidence for it. In this case, the procedure and the sanctions to be applied

will be those established in the legislation on the disciplinary or sanctioning regime that

be applicable.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Likewise, when the infractions are attributable to authorities and executives, and

accredit the existence of technical reports or recommendations for the treatment that

had not been duly attended to, in the resolution in which the

sanction will include a reprimand with the name of the responsible position and

will order the publication in the Official State or regional Gazette that

corresponds.

(…)

5. They will be communicated to the Ombudsman or, where appropriate, to similar institutions

of the autonomous communities the actions carried out and the resolutions issued

under this article."

In this case, it is deemed appropriate to sanction the party with a warning.

claimed, for violation of article 5.1.f) of the GDPR and for violation of article 32

of the GDPR, due to the lack of diligence when implementing the appropriate measures

of security with the consequence of the breach of the principle of confidentiality.

X

Measures

Article 58.2 of the GDPR provides: "Each control authority will have all the

following corrective powers indicated below:

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

treatment comply with the provisions of this Regulation, where appropriate,

in a specified manner and within a specified period;”

Likewise, it is appropriate to impose the corrective measure described in article 58.2.d) of the GDPR and order the claimed party to, within a month, establish the measures

Adequate security measures so that the treatments are adapted to the requirements

contemplated in articles 5.1 f) and 32 of the GDPR, preventing them from occurring if

similar situations in the future.

The text of the resolution establishes which have been the infractions committed and

the facts that have given rise to the violation of the regulations for the protection of

data, from which it is clearly inferred what are the measures to adopt, without prejudice

that the type of procedures, mechanisms or concrete instruments for

implement them corresponds to the sanctioned party, since it is responsible for the

treatment who fully knows its organization and has to decide, based on the

proactive responsibility and risk approach, how to comply with the GDPR and the

LOPDGDD.

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: SANCTION the DEPARTMENT OF

EDUCATION, CULTURE AND SPORTS, with NIF S5011001D, for an infraction of the

Article 5.1.f) of the GDPR, typified in Article 83.5 of the GDPR.

SECOND:

SANCTION the DEPARTMENT OF

EDUCATION, CULTURE AND SPORTS, with NIF S5011001D, for an infraction of the

Article 32 of the GDPR, typified in Article 83.4 of the GDPR.

THIRD: REQUEST the DEPARTMENT OF EDUCATION, CULTURE AND

SPORTS, which implements, within a month, the necessary corrective measures

to adapt its actions to the personal data protection regulations, which

prevent the repetition of similar events in the future, as well as to inform this

Agency within the same term on the measures adopted.

FOURTH: NOTIFY this resolution to the DEPARTMENT OF EDUCATION,

CULTURE AND SPORTS.

FIFTH: COMMUNICATE this resolution to the Ombudsman, in accordance

with the provisions of article 77.5 of the LOPDGDD.

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

938-181022

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es