 File No.: EXP202200993

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 December 15,

2021, filed a claim with the Spanish Agency for Data Protection. The re-

The complaint is directed against the MINISTRY OF EDUCATION AND PROFESSIONAL TRAINING.

GOVERNMENT OF THE BALEARIC ISLANDS, with NIF S0711001H (hereinafter,

the claimed party). The reasons on which the claim is based are the following:

The claimant states that during the 2020/2021 academic year, he was exercising

as a teacher at the IES IES.1, of ***LOCATION.1 (Illes Balears), being assigned

a corporate email address that you no longer had access to at the end of the

start the academic year. However, on December 15, 2021, he received communication

GOOGLE notification informing you of a new login to the aforementioned account

reason why he considers that his identity could have been supplanted and

your rights regarding data protection.

Next to the notification, it provides a screenshot of the message received from GOOGLE

alerting account login.

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 norm-

data protection tive.

The transfer, which was carried out by means of electronic notification, in accordance with the regulations

established in Law 39/2015, of October 1, of Administrative Procedure Co-

of the Public Administrations (hereinafter, LPACAP), was received on 4

February 2022, as stated in the acknowledgment of receipt in the file.

No response has been received to this letter of transfer.

THIRD: On March 15, 2022, in accordance with article 65 of the

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

complaining party.

FOURTH: The General Subdirectorate of Data Inspection proceeded to carry out

of previous investigative actions to clarify the facts in

matter, by virtue of the functions assigned to the control authorities in the

article 57.1 and the powers granted in article 58.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter GDPR), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the

LOPDGDD, having knowledge of the following extremes:

During these proceedings, the following entities have been investigated:

MINISTRY OF EDUCATION AND VOCATIONAL TRAINING OF THE GOVERNMENT OF

ILLES BALEARS, with NIF S0711001H, and address at CARRER DEL TER 16- 07009

PALMA (BALEARIC ISLANDS).

RESULT OF INVESTIGATION ACTIONS

The claimant provides a screenshot with content in Catalan in the

that GOOGLE reports that a new account login has occurred

***EMAIL.1.

On May 3, 2022, information was requested in relation to the facts

reported to the MINISTRY OF EDUCATION AND VOCATIONAL TRAINING

FROM THE GOVERNMENT OF THE BALEARIC ISLANDS, without obtaining a response.

On July 14, 2022, a response to the request for information from

the Data Inspection, in which the following is revealed:

The claimant has been a teacher at the center since September 1, 2020 until

on August 31, 2021.

During the first days of September, he was given an email address

corporate email, exclusively for academic and professional purposes

related to the mentioned educational center.

It has been detected that you have not accidentally withdrawn access to your email account

email in September 2021, as should have been done, that the

center has not changed the password of the email address of the

claimant, therefore, the claimant continued to have access to it.

The reasons and people who may have had access to this are unknown.

account, and that in no case has it been with the knowledge and consent of the team

manager, who at all times communicates to the teaching team that the use of this

account is exclusively for academic tasks, never for personal use, since it is

property of the educational administration, and that as a consequence of the detection

of the non-withdrawal of access to the corporate email account, the

access.

Regarding the required documentation on email security policies

corporate email, rules of use and information provided to employees and

users and cancellation rules for staff email accounts

unemployed, state that there is a security system called

double check. This system adds an additional layer of security in the event of

password theft and for security send an email to the same account

***URL.1 at the time it detects an input from a device other than the

usual. The system notifies the account holder with a message to verify that

it is not an intruder seeking undue access.

CONCLUSIONS:

-The claimant has been a teacher at the center since September 1, 2020 until

on August 31, 2021, and as a consequence an email address was provided

corporate email, exclusively for academic and professional purposes

related to the mentioned educational center.

-On December 15, 2021, there was an access to the corporate email account of the

claimant, ignoring the reasons and persons who may have had access

to this account.

-As a consequence of the detection of the non-withdrawal of access to the email account

corporate email, from this claim, access is withdrawn.

-Do not provide supporting documentation of email security policies

corporate email, rules of use and information provided to employees and

users and cancellation rules for staff email accounts

unemployed.

FIFTH: On November 23, 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 hereafter, LPACAP), for the alleged infringement of article 32 of the GDPR, typified in Article 83.4 of the GDPR.

The startup agreement was sent, in accordance with the rules established in the Law 39/2015, of October 1, of the Common Administrative Procedure of the Public Administrations (hereinafter, LPACAP), by means of electronic notification, being received on November 25, 2022, as stated in the certificate that work on file.

SIXTH: Notified the aforementioned start 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 provides a technical report prepared by the Information Technology in Education Service of the General Directorate of Early Childhood and Educational Community.

This report shows that, in the Balearic Islands, the centers educational have their own consoles either Google Workspace or Microsoft (in the case of a center), due to the need that arose during the pandemic to have digital environments in which to continue with the education of students before the confinement and semi-presentiality scenarios.

From the Ministry of Education and Vocational Training, through the CEP IBSTEAM, specific training was carried out for the management of these consoles

educational institutions in which the safety and protection policies of

data.

Likewise, it is indicated that, in the event of the leave for any reason of a worker, the

accounts are suspended, not deleted, so that if the worker is back in

active (frequent situation in teaching staff) can access emails

Electronics (with working documentation) from previous courses.

However, it is recommended that the time between termination and suspension of the account

is one month, although the educational centers applied a more lax policy in

regarding dates of suspension of users due to the implications of the pandemic of

COVID-19 allowing more time for teachers to transfer material to

new accounts.

In relation to the specific case that has generated the claim, it expresses its

surprise at the acceptance as evidence to process the complaint, of the capture of

screen of the email in which the date does not appear.

The Information Technology in Education Service, with the collaboration of the

IES center IES.1, have verified the activity of the account through the tools

audit and investigation of the Workspace console of the IES IES.1.

As a result of these verifications, it considers it necessary to take into account the

following:

-Despite what the claimant states, it is observed that there has been no

change of password. Neither the owner of the account ever made a change to this

from the moment of creation. Also, the only post-creation activity

of the account was its suspension dated June 15, 2022.

-The claimant, contrary to what he states, maintained access to the account until

June 2022. The educational centers applied a more lax policy regarding

User suspension dates due to the implications of the COVID-19 pandemic

allowing more time for teachers to transfer material to new accounts.

-Regarding access, there is an access dated December 15, 2021,

to perform the change of ownership of a Classroom class. This access is

made at the request of the claimant himself. When accessing the Classroom app, the

notice is produced in the same way as if you went directly to the application

mail.

-The center has a protocol for the use of corporate accounts for accounts

new, approved in September 2022. The original protocol and its

translation. Prior to this date the information was given orally.

Documentation accrediting the security policies is provided with this report

of corporate mail, which is being worked on at the Ministry level in addition to

those of the center.

SEVENTH: On February 6, 2023, a resolution proposal was formulated,

proposing:

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

GOVERNMENT MINISTRY OF EDUCATION AND VOCATIONAL TRAINING

OF THE BALEARIC ISLANDS, with NIF S0711001H, 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 February 6, 2023, as stated in the certificate that works

on the record.

EIGHTH: On February 14, 2023, the claimed party submitted a writ of

allegations to the Resolution Proposal, in which, in summary, it states that:

Regarding the first fact declared proven, in which the claimant considers that

Your identity could have been impersonated and your rights regarding the

data protection, alleges that it is a totally hypothetical manifestation, since

As stated in the Technical Report of February 13, 2023, the communication that

received by the complainant from Google on December 15, 2021, informing him of a

new login to your corporate account, it just proves that you received a notice of

security alert that an attempt to access the account had been detected

carried out automatically by Google and that from the analysis carried out on the console of the

IES IES.1, it was observed that this access attempt was produced by the action performed

by the claimant himself when making the change of ownership in the Classroom.

Therefore, there was only one access to his corporate account, which was on December 15.

of 2021, to make the change of ownership of a Classroom class, and this

access was made by the claimant himself. At no time has it been tested in the

disciplinary file that there was real access by another person to the account of the

claimant, nor that his identity has been supplanted.

Regarding the second fact declared proven, it states that the Service of

Information Technologies in Education with the collaboration of the IES center

IES.1, verified account activity using auditing tools and

investigation of the Workspace console of the IES IES.1, resulting that there was no

password change in the account from the moment of creation, by the user

user or administrator, and thus has been registered in the tool

Google Workspace console audit.

Regarding the third fact declared proven, it indicates that the non-suspension of the

claimant's account, which maintained access until June 2022, in no case

implies a security problem, since the technical measures of the

account.

It states that it should be taken into consideration that the Ministry of Education and

Vocational Training is applying continuous improvement measures regarding the

security and data protection policies. Thus, through the CEP IBSTEAM, they have

carried out specific training for the management of educational consoles

Workspace since 2020. In this specific case, the IES IES.1 approved a Protocol

use of the corporate account for faculty in September 2022, and

Currently, work is being done on the unification of all the consoles into one,

managed directly by the Information Technology Service in

Education.

It alleges that the fact that the Ministry is in an improvement process to

unifying the application of security measures is not equivalent to the previous situation

would imply a low level of security. Therefore, it can be said that these accounts

corporate email, whose use is exclusive for academic tasks by

be the property of the educational administration, are equipped with security systems

sufficient and efficient to prevent improper access by persons outside the

authorized in email accounts, by having double verification to

access from devices other than usual.

For all of the foregoing, it considers that the provisions of

article 32 of the GDPR, that despite having produced a security incident

in their systems, due to the fact that the claimant was not withdrawn access to their

email account as it should have been done, just like it happened with other

users in view of the difficulties of the situation derived from the COVID 19 pandemic, in

At no time during the processing of the disciplinary file have the

alleged facts that make up the infringement by the AEPD, and does not appreciate that

there is evidence to support access to this corporate account by a

third person, nor that their identity has been supplanted, and therefore, that

there has actually been an effective risk to the guarantees of the rights and

freedoms of the interested parties in relation to the processing of personal data, therefore

requesting that the disciplinary file be filed, with the consequent

declaration of absence of responsibility.

A Technical Report of the Information Technology Service is provided in the

Education, of February 13, 2023.

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 December 15, 2021, the claimant filed

his claim before the Spanish Data Protection Agency, in which he stated

manifest that during the 2020/2021 academic year, he was working as a professor

in the IES IES.1, of ***LOCALIDAD.1 (Illes Balears), being assigned an address

corporate email to which you no longer have access at the end of the course

academic.

However, on December 15, 2021, he received communication from GOOGLE, in-

forming a new login in the aforementioned corporate account for which

considers that their identity could have been impersonated and their rights violated in

around data protection.

SECOND: It is stated in the previous proceedings that the AEPD required the claimant to

information related to the incident, confirming what was stated in the study

claim, when stating the claimed party that accidentally was not

withdrew access to your email account as should have been done, and that

the center did not change the password of the claimant's email address

for which reason he continued to have access to it, unaware of the reasons and persons

who have been able to access the account.

THIRD: From the result of checking the activity of the account through

audit and investigation tools of the IES Workspace console IES.1,

carried out by the Service of Information Technology in Education, with the

collaboration of the IES IES.1 center, it is stated that the claimant who was a teacher at the

center from September 1, 2020 to August 31, 2021, maintained

access to the account until June 2022, that is, more than one month after the termination

of the claimant as a teacher at the center.

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."

II

previous questions

The Ministry of Education and Vocational Training of the Government of the Balearic Islands,

Like any other public entity, it is obliged to comply with the Regulation

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

to the protection of natural persons with regard to the processing of personal data.

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

December, 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.

In the specific case under review, the corporate email address

created in the context of work activity, composed of the name and surname of the

person to whom it has been attributed, constitutes personal data in the sense

do of article 4.1 of the GDPR, and, therefore, data related to a natural person

identified or identifiable.

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 above, the Ministry of Education and Vocational Training

of the Government of the Balearic Islands provides a series of public services, for which

it treats 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."

Regarding the application of data protection regulations to the alleged

raised, it should be taken into account that the GDPR, in its article 32, requires those responsible

responsible for the treatment, the adoption of the corresponding security measures

cesarean sections that guarantee that the treatment complies with current regulations, as well as

such as ensuring that any person acting under the authority of the controller or

of the person in charge and has access to personal data, can only process them following instructions

instructions of the person in charge.

Allegations Adduced to the Initiation Agreement

II

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

the next:

The defendant alleges that, in the event of a worker leaving for any reason, the

accounts are suspended, not deleted, so that if the worker is back in

active (frequent situation in teaching staff) can access emails

Electronics (with working documentation) from previous courses.

Likewise, the recommendation is indicated that the time between cessation and suspension of the account is one month, therefore, in this sense, it should be noted then that security measures were not being complied with at the time of the events.

From the result of checking account activity using tools audit and investigation of the Workspace console of the IES IES.1, carried out by the Information Technology in Education Service, with the collaboration of the IES center IES.1 states that the claimant, who was a teacher at the center from day 1 from September 2020 to August 31, 2021, you maintained access to the account until June 2022, that is, much more than a month after the claimant's termination as a teacher at the center.

From all this, it can be deduced a lack of due diligence both in compliance with the established security measures, as well as in the supervision or verification of its observance and/or suitability of these.

In fact, as stated in the previous proceedings, the AEPD required the re-claimed information related to the incident, confirming what was stated in the written claim, when stating the claimed party that accidentally was not withdrew access to your email account as should have been done, and that the center did not change the password of the claimant's email address for which reason he continued to have access to it, unaware of the reasons and persons who have been able to access the account.

In this regard, it should be noted that article 32 of the GDPR is infringed both if it is not the person in charge adopts the appropriate technical and organizational measures that guarantee the security of personal data, as if, established these, the they are not observed.

It is understood that the security measures implemented were insufficient,

capable of being improved; which is made clear by the statement that,

until September 2022, the center did not have a protocol for the use of the accounts

corporate for new accounts.

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.

IV.

Allegations Adduced to the Resolution Proposal

In response to the allegations presented by the respondent entity to the Proposal

Resolution, the following should be noted:

The claimed party alleges that there was only one access to the corporate account that was the

December 15, 2021, to make the change of ownership of a class of

Classroom, and this access was made by the claimant himself and that in no

moment it has been proven in the disciplinary file that there was a real access of

another person to the claimant's account, or that their identity has been impersonated.

Likewise, it states that there has been no password change in the account since the

time of creation, by the user or the administrator, and so it has been

logged in the Google Workspace console audit tool.

In this regard, it should be noted that the opening of this Proceeding

Penalty was not due to access to the corporate account by a third party

person, or that the identity of the claimant has been supplanted, but to the fact that

have been made aware that access to the account was maintained until June

2022, that is, much more than a month after the claimant's termination as a teacher

of the center, despite the fact that the recommendation was that the time between cessation and

suspension of the account outside of a month.

Thus, from the analysis of the documentation provided, the defendant herself acknowledges having

there has been a security incident in their systems, due to the fact that it was not withdrawn

claimant access to your email account as it should have been done,

as happened with other users in the face of the difficulties of the situation derived from the

COVID 19 pandemic. Moreover, it was after the claim, when the

access to the corporate email account.

In this sense, it should be remembered that 32 of the GDPR, stresses the need for

the controller takes appropriate technical and organizational measures

to effectively apply the data protection principles and guarantee a

level of security appropriate to the risk, without it being possible to accept as justification the

circumstance of the health emergency.

The defendant argues that the alleged facts that make up

the infraction. In this sense, it means that proactive responsibility entails

that those responsible and in charge have the obligation to comply with the GDPR and

demonstrate (prove) compliance with the GDPR in data processing

personal data, including the effectiveness of the measures, adequately documenting all

the decisions it adopts in order to prove it.

In this sense, Recital 74 establishes that:

"The responsibility of the data controller must be established for

any processing of personal data carried out by himself or on his behalf. In

In particular, the person responsible must be obliged to apply timely and effective measures

and must be able to demonstrate the compliance of the processing activities with the

this Regulation, including the effectiveness of the measures. These measures must have into account the nature, scope, context and purposes of the processing, as well as the risk to the rights and freedoms of natural persons."

In the specific case under review, it was found that the measures had not been adopted appropriate technical and organizational measures to ensure a level of security appropriate to the risk, since, until September 2022, the center did not have a protocol for the use of corporate accounts for new accounts. In fact, Prior to this date, the information was given orally.

By continuing to access the email account, you continue to be able to access personal data and information to which you should no longer have access for not

work in that center. This risk must be taken into account by the person in charge of the treatment who must establish the necessary technical and organizational measures and that increases the requirement of the degree of protection in relation to safety and security save this data.

As regards the continuous improvement measures that the Ministry claims to have adopted in terms of security and data protection policies, although it reflects positive conduct, does not distort the facts verified and that are constitutive of an infraction, attributable to the claimed party, for violation of article 32 GDPR.

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.

V

GDPR Article 32

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

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

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

and variable severity for the rights and freedoms of natural persons, the responsibility

responsible and the person in charge of the treatment will apply appropriate technical and organizational measures.

measures to guarantee a level of security appropriate to the risk, which, where appropriate, will include

yeah, among others:

to)

to)

to)

pseudonymization and encryption of personal data;

the ability to ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

the ability to restore availability and access to personal data

quickly in the event of a physical or technical incident;

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

technical and organizational measures to guarantee the safety of the

treatment.

2. When assessing the adequacy of the security level, particular account shall be taken of

The risks presented by the data processing, in particular as a consequence

of the destruction, loss or accidental or illegal alteration of personal data transmitted

collected, preserved or processed in another way, or the unauthorized communication or access

two to said data.

3. Adherence to a code of conduct approved under article 40 or to a mecha-

certification document approved in accordance with article 42 may serve as an element to

demonstrate compliance with the requirements established in section 1 of this

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 having

ga access to personal data can only process such data following instructions

of the controller, unless it is required to do so by Union law or by

the Member States".

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:

"Risks to the rights and freedoms of natural persons, serious and pro-

Variable reliability may be due to data processing that could cause damage.

physical, material or immaterial damages and damages, particularly in cases in which

the treatment may give rise to problems of discrimination, identity theft

or fraud, financial loss, damage to reputation, loss of confidentiality of

data subject to professional secrecy, unauthorized reversal of pseudonymization or

any other significant economic or social damage; in the cases in which the

prevents the interested parties from their rights and freedoms or prevents them from exercising control over

open your personal data; in cases in which the personal data processed reveals

regardless of ethnic or racial origin, political opinions, religious or philosophical beliefs,

union membership and the processing of genetic data, data relating to health or

data on sexual life, or criminal convictions and offenses or security measures

related ity; in cases where personal aspects are evaluated, in particular

the analysis or prediction of aspects related to performance at work, situation

economics, health, personal preferences or interests, reliability or behavior,

situation or movements, in order to create or use personal profiles; In the cases

in which personal data of vulnerable persons, in particular children, are processed; either

in cases where the processing involves a large amount of personal data

and affects a large number of stakeholders."

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

The claimed party has violated article 32 of the GDPR, when an incident of

security in their systems, by not withdrawing access to the claimant's email account

email as it should have been done.

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

security measures that are applicable in accordance with 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 in the

treatment, taking into account the state of the art, the costs of application, the na-

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

detected risk, noting that the determination of technical and organizational measures

must be carried out taking into account: pseudonymization and encryption, the capacity

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

capacity to restore availability and access to data after an incident, recovery process

verification (not audit), evaluation and assessment of the effectiveness of the measures.

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

take into account the risks presented by data processing, as a consequence

of the destruction, loss or accidental or illegal alteration of personal data transmitted

collected, preserved or processed in another way, or the unauthorized communication or access

to said data and that could cause physical, material or in-

materials.

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

"(83) In order to maintain security and prevent processing from infringing the provisions of

this Regulation, the controller or processor must assess the risks

inherent to the treatment and apply measures to mitigate them, such as encryption. Are you-

measures must ensure an adequate level of security, including confidentiality,

taking into account the state of the art and the cost of its application with respect to

the risks and nature of the personal data to be protected. When evaluating the

risk in relation to data security, the risks should be taken into account

derived from the processing of personal data, such as destruction, loss or

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

otherwise, or unauthorized communication or access to said data, susceptible

in particular of causing physical, material or immaterial damages.

In the present case, as stated in the previous proceedings, the AEPD required the

the requested party information related to the incident, confirming what was indicated

stated in the claim document, when stating the claimed party that accidentally

access to your email account was not removed as should have been done

cho, and that the center did not change the password of the email address of the

claimant for which reason he continued to have access to it, unaware of the reasons

and people who have been able to access the account.

The liability of the claimed party is determined by the insurance bankruptcy.

revealed in the claim and documentation provided, since it is res-

responsible for making decisions aimed at effectively implementing the

appropriate technical and organizational measures to ensure a level of safety

appropriate to the risk to ensure the confidentiality of the data, restoring its distribution

availability and prevent access to them in the event of a physical or technical incident.

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

infringement, attributable to the claimed party, for violation of article 32 GDPR.

Classification of the infringement of article 32 of the GDPR

SAW

The aforementioned infringement of article 32 of the RGPD supposes the commission of infringements ti-

classified 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 a maximum of 10,000,000 EUR or, in the case of

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

overall annual total business of the previous financial year, opting for the one with 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 "Consti-

The acts and behaviors referred to in sections 4, 5 and 6 have infractions

of 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 73 "Infractions considered serious"

of the LOPDGDD indicates:

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

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

substantial portion of the articles mentioned therein and, in particular, the following:

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

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

treatment, in the terms required by article 32.1 of the Regulation (EU)

2016/679."

VII

Responsibility

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."

The lack of adoption of technical and organizational measures that are appropriate for

guaranteeing a level of security appropriate to the risk of the treatment constitutes the element

moment of guilt

VIII

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 art.

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

of, and to what extent, imposing administrative fines on public authorities and bodies

public establishments established in that Member State."

Likewise, article 77 "Regime applicable to certain categories of liability"

responsible or responsible for 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 autonomous communities,

tonomas and 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 organic law

only, the data protection authority that is competent will issue a resolution

sanctioning them with warning. The resolution will also establish the

measures that should be adopted to cease the conduct or to correct the effects of the

offense that was 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 in-

Sayings enough for that. 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.

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 corresponding Official State or regional Gazette.

gives.

4. The data protection authority must be informed of the resolutions that

fall in relation to the measures and actions referred to in the sections

previous.

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.

6. When the competent authority is the Spanish Data Protection Agency,

This will publish on its website with due separation the resolutions referring to

the entities of section 1 of this article, with express indication of the identity

of the person in charge or in charge of the treatment that had committed the infringement.

When the competence corresponds to an autonomous authority for the protection of

data will be, in terms of the publicity of these resolutions, to what your

specific regulations."

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

claimed, for the infringement of article 32 of the GDPR, for the lack of adoption of

those technical and organizational measures that are appropriate to guarantee a

level of security appropriate to the risk of the treatment.

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 MINISTRY OF EDUCATION with a WARNING

AND PROFESSIONAL TRAINING OF THE GOVERNMENT OF THE BALEARIC ISLANDS, with

NIF S0711001H, for a violation of article 32 of the GDPR, typified in article

83.4 of the GDPR.

SECOND: NOTIFY this resolution to the MINISTRY OF EDUCATION AND

VOCATIONAL TRAINING OF THE GOVERNMENT OF THE BALEARIC ISLANDS.

THIRD: COMMUNICATE this resolution to the Ombudsman, in

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

C / Jorge Juan, 6

28001 – Madrid

938-181022

www.aepd.es

sedeagpd.gob.es