 File No.: EXP202201318

RESOLUTION OF TERMINATION OF THE PROCEDURE FOR PAYMENT

VOLUNTEER

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

to the following

BACKGROUND

FIRST: On March 23, 2023, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against BARNA PORTERS

SEGURETAT, S.L. (hereinafter, the claimed party), through the Agreement that

transcribe:

<<

File No.: EXP202201318

AGREEMENT TO START THE SANCTION PROCEDURE

Of the actions carried out by the Spanish Data Protection Agency and in

based on the following

FACTS

FIRST: D.A.A.A. (hereinafter, the claiming party), on December 27,

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

claim is directed against BARNA PORTERS SEGURETAT, S.L. with NIF

B62735089 (hereinafter, the claimed party). The reasons on which the claim is based

are the following:

In the letter received by this Agency, a vulnerability is reported on the website

of the company BARNA PORTERS SEGURETAT, S.L., existing for a year.

As explained, by clicking with the mouse on an icon in the shape of a red magnifying glass that

appears in the upper left corner of the screen corresponding to the section

"Accés Serviap", (whose link can be found at the bottom of the aforementioned web page),

an Excel file of authorizations for

Covid-19, with (...) entries, containing the following information: (...).

The Inspection services of this Agency have verified that, at the time of

submission of the claim, the vulnerability continued to exist.

Along with the claim, provide a complete Excel file containing authorizations for

Covid-19, with (...) tickets and set of images to explain how to access

such information.

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 means of electronic notification, was received in

dated February 11, 2022, as stated in the certificate in the file.

On March 11 and 16, 2022, this Agency received a written response

indicating that the notification sent by the Agency is the first communication

received by which they are aware of the reported violation, not having

received prior communication from the complainant or from any other possible affected party.

It states that SERVIAP, as an intranet or internal tool of the company, is a

private tool, custom developed by ENDURO WEB TOURS SL with CIF

B66390725 (in charge of the treatment), hereinafter ENDURO, to which they only have

access authorized users (through username and password), so it is not

accessible to people without ties to the company.

No one unrelated to or outside the company can have access to this personal data,

with the exception, obviously, of the reported incident, caused by an error in

programming during the development of some tests of the new version of the intranet

corporate. It indicates that to date no complaints have been received from

no person about said circumstance.

It explains that the cause that has caused the claim has been a failure of

programming:

- Your computer provider, ENDURO, is the same one that develops the application

SERVIAP as an internal intranet tool of the company, to which they have access

Workers. This application has been developed to measure.

- At the time, complying with the obligation to provide workers with a

“Covid-19 self-responsibility certificate”, a form was scheduled

auto-fill authorization form for personnel movement during restricted hours

COVID-19.

Said form was only accessible to registered users, workers of the

company, not containing personal data, until it was filled in by the

workers, so the data entered has been provided by the

own users.

The personal data, consisting of (...) were stored in a database

data.

It is this database, which fed the file that was accessed

accidental in the Serviap logo icon that appears in the upper left part of the

access page https://serviap.cat/ during tests of a new version of

Serviap.

- Since they were working on a more advanced version with more

Serviap functionalities to replace version v19.51, at the end of 2021, will be

carried out some programming tests, feeding the database with the

list that could be accessed accidentally as indicated with

anteriority.

The “red magnifying glass” icon at the top left of the page

of access to SERVIAP, where the vulnerability was detected, it is not about any

search tool, but said icon corresponds to the logo of the application,

so it is not operational or contains access for users.

It exposes that the vulnerability has been caused by a programming error in one of the

computer technicians (junior programmer) who accidentally inserted a link

that allowed the file to be downloaded.

The list, which has given rise to the complaint, has been removed from the link

accidental, once knowledge of said circumstance has been made, that is, at the

receipt of the requirement formulated by the Agency, on February 11,

currents.

Said icon (the logo of the application) has never been designed or designated as a

access to the tool, not being the object of access to a database

public or information with the exception of being only the identifying logo of

the corporate intranet.

Indicates that once the vulnerability was communicated and verified, ENDURO reviewed the

home page of the intranet and immediately proceeded to remove the link that

accidentally gave access to the list, so said vulnerability was

removed.

Both from the organization and the data protection delegate of this

were able to verify that said vulnerability was annulled and that it was no longer possible

access the file that same afternoon.

Regarding the measures adopted by the person in charge to solve the aforementioned

situation have been:

a) Contact the provider in charge of programming and maintaining the

corporate intranet to remove immediately, the accidental link in the

icon (logo of the intranet) that appears in the upper left part of the page of

access to Serviap.

b) Register the reported violation in the Incident Register.

c) Debug the excel file to know the number and people affected.

d) Inform users through a notice on the intranet itself.

As for the measures adopted to avoid a repetition of this situation, they have been:

a) Reiterate to the person in charge of the treatment the obligations in terms of protection

of data.

b) Request the transfer of the direction and supervision of programming,

maintenance and testing of the Serviap intranet to a senior programmer with

more years of experience. In this regard, it is worth noting the commitment by

part of Enduro, which has agreed to entrust these tasks to a

Senior programmer with more than years of experience.

In turn, it is indicated that you should avoid testing with real data.

The data affected by the detected violation consist of: (…).

Indicates that the file accessible through the reported vulnerability contained (...)

entries, many of them repeated and that, once the repetitions have been refined, and

subtracted the header line, the user "Demo" and the user "No Vale" are

confirms a total of (...) people affected without including any

minor.

Since access to the company's intranet page https://serviap.cat/ is

carried out mainly, if not exclusively, by the staff of the organization,

the incidence or possible consequences for the people affected are estimated to be low.

Regarding the communication of the incident to the AEPD, he states that, since the

responsible has become aware of said violation through the notification

sent by the Spanish Data Protection Agency itself, the organization has not

considered necessary to notify the gap to the AEPD in accordance with art. 33 GDPR, at

already have knowledge of this, since it was the authority itself who communicated to the

organization the vulnerability detected.

Finally, it indicates that the organization is firmly committed to the

regulatory compliance not only in the areas where it provides its services: surveillance of

facilities and protection of goods, establishments, shows, contests or

conventions, custody of keys and receipts, operation of reception center of

alarms, protection of people and installations and maintenance of devices and

security devices; but with continuous improvement and quality standards.

In connection with the above statements, the Respondent provides the

following documentation:

- Document number ONE detailing the "Labor and HR" treatment, where

You can appreciate, among others:

or file structure,

or principles of treatment,

or security policy, and

or data protection measures.

- Document number TWO: refined Excel file, containing the list of the

people affected and arranged alphabetically.

- Document number THREE: Report issued by the Delegate for the Protection of

Data about the incident.

- Document number FOUR: ISO 27001 Certificate

- Document number FIVE: Final Audit Report 2021, ISO 27001 where

You can see that on 05.15.2021 no incident was detected, nor was there any

any findings that would point to the reported vulnerability.

THIRD: On March 27, 2022, in accordance with article 65 of the

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

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

of previous investigative actions to clarify the facts in

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

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

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:

INVESTIGATED ENTITIES

BARNA PORTERS SEGURETAT, S.L. with NIF B62735089 with address in ARIZALA,

43 - 08028 BARCELONA (BARCELONA)

ENDURO WEB TOURS SL with NIF B66390725 with address at C/ BRUC, 3. - 08758

CERVELLO (BARCELONA)

RESULT OF INVESTIGATION ACTIONS

On June 16, 2022, it is verified that the link to download the file

from the website https://serviap.cat has disappeared.

On June 16, 2022, it was verified that a web page https://

serviap.cat/21serviap.asp under development. It is saved in the SIGRID system, as an object

associated, the screenshot of the home page of this website under development.

Following the request for additional information required by this Agency to

BARNA PORTERS dated July 7, 2022, the claimed party refers to this

Agency, with entry registration number in the AEPD REGAGE22e00032239897 and

dated July 26, 2022, the following documentation:

- Record of processing activities

- Log of security violations

- Treatment manager contract with CLAU informática

- Treatment manager contract with LEITIC

- Treatment manager contract with ENDURO

- Completion form for treatment managers/suppliers

- Confidentiality agreement for suppliers

- GDPR compliance guarantee certificate

It is verified that the Record of processing activities provided by the

The claimed party contains all the information that article 30 of the Article 30 of the

GDPR.

The Security Violation Log is analyzed, verifying that the security violation has been included.

Incident produced on February 11, 2022 along with all the necessary information

to treat it:

- Type of incident

- Person who reports the incident

- Person in charge of resolution

- Affected files

- Description

- Effects caused

- Corrective measures

This record details that, having been informed by the workers through

notice on the corporate intranet, no claim has been filed by

those affected as of March 10, 2022.

The corrective measures specified in the registry are the following:

- 1:37 p.m. Incident has been reported to DPD.

- 1:38 p.m. The data manager responsible for programming has been contacted

and maintenance of the website. You are informed of the reported vulnerability and

requires proceed to review and take the appropriate corrective measures to cancel

the automatic download of the file by clicking on the icon in the upper corner

left.

- 14.02h The accidental link that allowed the download of the file has been removed.

- 2:07 p.m. The DPD is informed of the elimination of the vulnerability

- 2:16 pm ENDURO is contacted again:

a) the data protection obligations have been reiterated

as ET and are reminded that testing with data should be avoided.

real.

b) has been asked to direct and supervise the programming,

maintenance and testing of the Serviap intranet is assigned to a programmer

senior with more years of experience.

Such issues are accepted by the provider.

The defendant states in his brief that, after the communication of the vulnerability

detected by the AEPD on February 11, 2022 and its resolution of

almost immediately, it was published on February 14, 2022 on the intranet

notice about the incident detected.

Managers and roles

In its response brief, the claimed party continues to state the roles

performed by the different suppliers with whom they maintain contracts of

treatment managers and attach a copy of said contracts.

Regarding ENDURO, he specifies that it is his IT provider: he deals

both the maintenance of systems and applications, as well as the development of the

SERVIAP application as an internal intranet tool of the company, to which

workers have access

Reviewed the contract between BARNA PORTERS, as data controller, and

ENDURO, as Data Processor, notes that in said contract it is

take into account the aspects specified in article 28.3 of the GDPR.

. - Object, duration, nature and purpose of the treatment.

. - Type of personal data and categories of interested parties.

. - Obligations and rights of the person in charge.

. - Obligations and rights of the Manager.

This section includes the obligation to process personal data only

for the end of the order.

. - Personnel authorized to carry out the treatment.

In this section, the person in charge guarantees that the staff has received the training

necessary to ensure that data protection will not be jeopardized

personal.

In this regard, it will be seen later that ENDURO has provided a certificate

training in data protection for the personnel of your company authorized to

the processing of personal data.

. - Security measures.

In this section, the MANAGER declares to be up to date with regard to

the obligations derived from the Data Protection regulations, especially in

regarding the implementation of security measures for the different

categories of data and treatment established in article 32 of the GDPR.

The MANAGER guarantees that said security measures will be adequately implemented.

security and will help the person responsible to comply with the obligations established in the

articles 32 to 36 of the GDPR.

. - Security breach.

. - Communication of data to third parties.

. - International data transfers.

. - Outsourcing of data processing.

. - Rights of the interested parties.

This section specifies assistance to the person in charge, whenever possible,

in attention to the exercise of rights of the interested parties.

. - Responsibility

. - End of service provision.

It is specified that, at the choice of the person in charge, the person in charge must delete or

return the stored data.

ENDURO suitability as developer and commissioner

Consulted the claimed party about the characteristics and suitability of ENDURO for

carry out the development of the SERVIAP application, BARNA PORTERS explains why

considers that this company offers sufficient guarantees as manager to apply

appropriate technical and organizational measures and justifies it by providing the following

documentation:

. - Completion form for treatment managers/suppliers

. - Confidentiality agreement for suppliers

. - GDPR compliance guarantee certificate

On July 7, 2022, information is requested from ENDURO.

On that same date, the notification is made available to you through the

electronic notifications Notific@, in which the date of automatic rejection is stated: 18

July 2022.

Said request is reiterated through the postal services, this notification being

delivered on August 2, 2022.

Dated August 12, 2022 and with AEPD entry registration number

REGAGE22e00035200405, ENDURO sends this Agency the following information and

manifestations:

Development methodologies and test protocol

Asked about the development methodologies that ENDURO follows in a project

of these characteristics and the development and testing protocols before carrying out a

new version to production, ENDURO explains in detail the needs,

application requirements, architectures, and functionalities, along with the lifecycle

(including test methodology) and the treatment of data in the different

application layers.

Those responsible for the project carry out a series of tests to confirm the

feasibility and utility of the solution. If it complies with what was established in the design phase,

It is implemented in processes that require it. If not, action should be taken

to correct the failures that prevent its normal development.

Required the catalog of tests that have been carried out before deploying the

new version of SERVIAP in production (that is, in particular for this case of

development of a new version of SERVIAP), ENDURO does not provide particular evidence

for this matter.

Technical qualification of personnel

Regarding the technical qualification of the people involved in the project of

development, ENDURO goes on to specify the technical profiles that have been involved

in each part of the project. Figures such as analyst, designer, programmer intervene

and trainer.

Data protection training

In this sense, ENDURO details that it conducts training on an annual basis and

provides a data protection training certificate in which

specifies, among other things, that ENDURO has received adequate information and

sufficient to adapt and keep up to date with the GDPR and to transmit it to the

authorized personnel for the processing of personal data

File origin of the breach and accidental link

Consulted about the purpose of creating the breach source file, ENDURO

states that, due to travel restrictions and curfew due to

of the COVID-19 epidemic, it was necessary to implement a form for staff

of the company

The information contained in this file facilitated confirmation to third parties,

mainly security forces and bodies and exceptionally (for security) to

end customer that the posted worker traveled to cover a

determined position/location.

ENDURO declares that, during the development of the new version of the intranet
corporate, it seems that one of the programmers accidentally pasted by mistake
the internal access link to the file in the logo of the intranet access page
corporate, at the end of November, beginning of December 2021.

Recurrence of incidents and vulnerabilities

ENDURO concludes by highlighting that the accidental link was removed in a manner
immediately as soon as it became known and that this is the first incident to
that the company has faced.

CONCLUSIONS

Confidentiality security breach caused by a programming error that
allows the download of an Excel file containing personal data of the
company workers.

The defendant BARNA PORTERS acknowledges that the access link to the file was pasted
by mistake in the logo of the access page to the corporate intranet.

ENDURO places the pasting of the link at the end of November, beginning of December
of 2021.

The accidental link was removed immediately as soon as it became known
of it. The breach was fixed on February 11, 2022.

The availability and integrity of personal data are not affected, since
that this link allowed the download of the file, but not the modification of the file in
your server.

The measures taken by the controller to fix the breach are considered
suitable.

The complained party has informed users through a notice on the intranet,
Posted on the first business day after learning of the breach.

The claimed party did not notify the AEPD of the breach since it was the AEPD itself

who informed the organization of the vulnerability detected.

The treatment manager contract between BARNA PORTERS, as responsible

of the treatment, and ENDURO, as the person in charge of the treatment, takes into account the

aspects specified in article 28.3 of the GDPR.

In particular, the security measures section indicates that the MANAGER

declares to be up-to-date with regard to the obligations derived from the

Data Protection regulations, especially with regard to the

implementation of security measures.

ENDURO has provided information on the test protocols that are carried out

carried out before bringing a new version to production, but has not provided

evidence of the tests that have been carried out in this particular case.

Although the programming error that caused the security breach is

unlikely that it would have been detected in a battery of tests (since it is not

functionality being implemented), ENDURO has not provided

evidence that confirms that in this case the battery of tests has been carried out

before taking the version to production.

FIFTH: According to the report collected from the AXESOR tool, the entity

BARNA PORTERS SEGURETAT, S.L. It is a large company established in the year

2001, (…).

FUNDAMENTALS OF LAW

Yo

Competence

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

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

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

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

Guarantee of Digital Rights (hereinafter, LOPDGDD), is competent to

initiate and resolve this procedure, the Director of the Spanish 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

BARNA PORTERS SEGURETAT, S.L. is a company with the legal form of a company

limited dedicated to private security activities, for which it processes personal data

personal character of its clients and workers, understanding by personal data

nal: “any information about an identified or identifiable natural person”.

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

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”.

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
caused by a programming error that allowed the download of an Excel file
that contained personal data of the company's workers.

The data affected by the detected violation were: (…). They were not affected

the availability or integrity of personal data, since the link allowed

downloading the file, but not modifying the file on your server.

The file accessible through the reported vulnerability contained (...) entries,

many of them repeated, although, once the repetitions are refined, a

total of (...) people affected without including any minor.

Since access to the company's intranet page is done

mostly, if not exclusively, by the staff of the organization,

estimated the incidence or possible consequences for the people affected to be low.

The accidental link was removed immediately as soon as it became known

of it. The breach was fixed on February 11, 2022.

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

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

themselves.

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.

II

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 party

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

time that, as a result of the confidentiality breach, the personal data of (...) people

workers in the file were unduly exposed to third parties, violating the

principles of integrity and confidentiality, both established in the aforementioned article

5.1.f) of the GDPR.

The data affected by the detected violation were: (…).

In accordance with the evidence available at the present time of

agreement to start the disciplinary procedure, and without prejudice to what results from the

investigation, it is considered that the known facts could constitute a

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

IV.

If confirmed, the aforementioned violation of article 5.1.f) of the GDPR could lead to the

commission of the offenses typified in article 83.5 of the GDPR that under the

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. (…)”

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, 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 and organizational measures by enabling the display of personal data of registered users two, employees of the company, with the consequent lack of diligence for the responsibility saber, allowing unauthorized access by outside parties. The person in charge of the The treatment maintains that the vulnerability was caused by a programming error during the development of tests of the new version of the corporate intranet, by one of computer technicians (junior programmer) who accidentally inserted a link that allowed the file to be downloaded.

At the time, complying with the obligation to provide workers with a "Covid-19 self-responsibility certificate", a form was scheduled auto-fill authorization form for personnel movement during restricted hours COVID-19.

In principle, said form was only accessible to registered users, employees of the company, not containing personal data, until it was filled in by the workers themselves.

From the analysis of the documentation provided by the claimed party, it turns out that it was this

database, the one that fed, with real data, the file that was accessed

accidental. This scenario represents a great risk that may end up favoring

the leakage of information to third parties. The risk is found precisely when

use real data of those people who were in the database of the

productive environment - a place where they were safe - and they move to the environment of

test where they are most vulnerable. Hence, you must ensure that the data is

replaced by others, so that they can be used in test environments,

with the certainty that the tests are valid, while guaranteeing the protection

of confidential data so that, if it were to leak, there is no

possibility of relating them to the real people in question. It is a measure of

Basic security, reflecting the principle of privacy by design and by default.

Likewise, it is clear that, although the programming error that caused the breach of

security is unlikely to have been detected in a battery of tests, the

person in charge of the treatment has not provided evidence that confirms that in this

If the battery of tests has been carried out before taking the version to production.

The testing phase is a necessary and very important process that, if carried out

correctly, constitutes another security measure that allows obtaining results

reliable, being of great benefit for the company in question to operate in a

more efficient.

In this sense, the person in charge of the treatment has committed to order said

work to a senior programmer with more than years of experience.

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, (...) 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 do not
they have to have been consented to by the 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

In this sense, Recital 74 of the GDPR 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."

Transferring these considerations to the specific case under examination, it can be

conclude that, at the time of the breach, the claimed party did not have

of the reasonable security measures based on the possible estimated risks,

since the defendant herself acknowledges that the access link to the file was pasted

by mistake in the logo of the access page to the corporate intranet by one of the

computer technicians (junior programmer) having since applied for the

transfer of management and supervision of programming, maintenance and testing of

the Serviap intranet to a senior programmer with more years of experience.

In accordance with the evidence available in this agreement of

initiation of the disciplinary procedure, and without prejudice to what results from the

investigation, it is considered that the known facts could constitute a

infringement, attributable to the defendant, for violation of article 32 of the GDPR

Classification of the infringement of article 32 of the GDPR

SAW

If confirmed, the aforementioned infringement of article 32 of the GDPR could lead to the

commission of the offenses typified in article 83.4 of the GDPR that under the

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.”

VII

Sanction proposal

In order to determine the administrative fine to be imposed, the

provisions of articles 83.1 and 83.2 of the GDPR, precepts that state:

"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, in addition to or in lieu of the measures contemplated in

Article 58, paragraph 2, letters a) to h) and j). When deciding to impose a fine

administration and its amount in each individual case shall be duly taken into account:

a) the nature, seriousness and duration of the offence, taking into account the nature

nature, scope or purpose of the processing operation in question, as well as the number

number of interested parties affected and the level of damages they have suffered;

b) intentionality or negligence in the infraction;

c) any measure taken by the person in charge or in charge of the treatment to

settle the damages suffered by the interested parties;

d) the degree of responsibility of the person in charge or of the person in charge of the treatment, habi-

gives an account of the technical or organizational measures that have been applied by virtue of the

articles 25 and 32;

e) any previous infringement committed by the controller or processor;

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

infringement and mitigate the possible adverse effects of the infringement;

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

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

determine whether the controller or processor notified the infringement and, if so, to what extent

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

given previously against the person in charge or the person in charge in relation to

the same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or to certification mechanisms.

fications approved in accordance with article 42,

k) any other aggravating or mitigating factor applicable to the circumstances of the case,

as the financial benefits obtained or the losses avoided, directly or indirectly.

mind, through infraction."

For its part, article 76 "Sanctions and corrective measures" of the LOPDGDD

has:

"1. The sanctions provided for in sections 4, 5 and 6 of article 83 of the Regulation

(UE) 2016/679 will be applied taking into account the graduation criteria

established in section 2 of said article.

2. In accordance with the provisions of article 83.2.k) of Regulation (EU) 2016/679

may also be taken into account:

a) The continuing nature of the offence.

b) 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

data.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

cases in which there are controversies between those and any

interested."

Penalty for violation of article 5.1.f) of the GDPR

In accordance with the transcribed precepts, and without prejudice to what results from the

instruction of the procedure, for the purpose of setting the amount of the sanction for infringement

of article 5.1 f) of the GDPR, to the party claimed as responsible for said

offense typified in article 83.5 of the GDPR, it is appropriate to graduate the fine taking into account

consider:

As aggravating factors:

Article 83.2 a) the nature, seriousness and duration of the infringement, taking into account

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

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

have suffered; for not having duly guaranteed, at least between the end of

November and early December 2021, the confidentiality of the data of (...)

affected people. The defendant herself acknowledges that the access link to the file

It was pasted by mistake in the logo of the access page to the corporate intranet.

Considering the exposed factors, the initial assessment that reaches the amount of the

fine is €20,000 for violation of article 5.1 f) of the GDPR, regarding the

breach of the principle of confidentiality.

Penalty for violation of article 32 of the GDPR

In accordance with the transcribed precepts, and without prejudice to what results from the

instruction of the procedure, for the purpose of setting the amount of the sanction for infringement

of article 32 of the GDPR, to the party claimed as responsible for said

offense typified in article 83.4 of the GDPR, it is appropriate to graduate the fine taking into account

consider:

As aggravating factors:

Article 83.2 a) the nature, seriousness and duration of the infringement, taking into account

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

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

have suffered; for not having duly guaranteed, at least between the end of

November and early December 2021, the confidentiality of the data of (...)

affected people. The defendant herself acknowledges that the access link to the file

It was pasted by mistake in the logo of the access page to the corporate intranet.

Considering the exposed factors, the initial assessment that reaches the amount of the

fine is €10,000 for violation of article 32 of the GDPR, regarding the lack of

diligence in implementing appropriate security measures.

Therefore, in accordance with the foregoing, by the Director of the Agency

Spanish Data Protection,

HE REMEMBERS:

FIRST: INITIATE SANCTION PROCEDURE against BARNA PORTERS

SEGURETAT, S.L., with NIF B62735089,

- For the alleged infringement of article 5.1.f) of the GDPR, classified in accordance with the provided in article 83.5 of the GDPR, classified as very serious for the purposes of prescription in article 72.1 a) of the LOPDGDD.

- for the alleged infringement of article 32 of the GDPR, classified in accordance with the provisions in article 83.4 of the GDPR, classified as serious for the purposes of prescription in the Article 73 f) of the LOPDGDD.

SECOND: APPOINT instructor to B.B.B. and, as secretary, to C.C.C., indicating that any of them may be challenged, where appropriate, in accordance with the provisions of Articles 23 and 24 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector (LRJSP).

THIRD: INCORPORATE into the disciplinary file, for evidentiary purposes, the claim filed by the claimant and its documentation, the documentation provided by BARNA PORTERS SEGURETAT, S.L., with NIF B62735089, as well as the documents obtained and generated by the Subdirectorate General of Data Inspection in the actions prior to the start of this sanctioning procedure.

FOURTH: THAT for the purposes provided for in art. 64.2 b) of Law 39/2015, of 1 October, of the Common Administrative Procedure of Public Administrations, the sanction that could correspond would be, for the alleged violation of article 5.1.f) of the GDPR, typified in article 83.5 of said regulation, an administrative fine of amount 20,000.00 euros and for the alleged violation of article 32 of the GDPR, typified in article 83.4 of said regulation, administrative fine amounting to 10,000.00 euro.

FIFTH: NOTIFY this agreement to BARNA PORTERS SEGURETAT, S.L., with NIF B62735089, granting a hearing period of ten business days so that Formulate the allegations and present the evidence that you consider appropriate. In its

pleadings must provide your NIF and the procedure number that appears

at the top of this document.

If, within the stipulated period, he does not make allegations to this initial agreement, the same

may be considered a resolution proposal, as established in article

64.2.f) of Law 39/2015, of October 1, on the Common Administrative Procedure of

Public Administrations (hereinafter, LPACAP).

In accordance with the provisions of article 85 of the LPACAP, you may recognize your

responsibility within the period granted for the formulation of allegations to the

present initiation agreement; which will entail a reduction of 20% of the

sanction that should be imposed in this proceeding. With the application of this

reduction, the sanction would be established at 24,000.00 euros, resolving the

procedure with the imposition of this sanction.

In the same way, it may, at any time prior to the resolution of this

procedure, carry out the voluntary payment of the proposed sanction, which

will mean a reduction of 20% of its amount. With the application of this reduction,

the sanction would be established at 24,000.00 euros and its payment will imply the termination

of the procedure, without prejudice to the imposition of the corresponding measures.

The reduction for the voluntary payment of the penalty is cumulative to the corresponding

apply for acknowledgment of responsibility, provided that this acknowledgment

of the responsibility is revealed within the period granted to formulate

allegations at the opening of the procedure. Voluntary payment of the referred amount

in the previous paragraph may be done at any time prior to the resolution. In

In this case, if both reductions were to be applied, the amount of the penalty would remain

established at 18,000.00 euros.

In any case, the effectiveness of any of the two aforementioned reductions will be

conditioned to the withdrawal or resignation of any action or appeal via

administrative against the sanction.

In the event that you choose to proceed with the voluntary payment of any of the amounts

previously indicated (24,000.00 euros or 18,000.00 euros), you must make it effective

by entering the account number IBAN: ES00-0000-0000-0000-0000-0000

(BIC/SWIFT Code: CAIXESBBXXX) opened in the name of the Spanish Agency for

Protection of Data in the banking entity CAIXABANK, S.A., indicating in the

concept the reference number of the procedure that appears in the heading

of this document and the reason for the reduction of the amount to which it accepts.

Likewise, you must send proof of income to the General Subdirectorate of

Inspection to continue with the procedure in accordance with the quantity

entered.

The procedure will have a maximum duration of nine months from the

date of the initiation agreement or, where appropriate, of the draft initiation agreement.

After this period, its expiration will occur and, consequently, the file of

performances; in accordance with the provisions of article 64 of the LOPDGDD.

In compliance with articles 14, 41 and 43 of the LPACAP, it is noted that, as regards

successively, the notifications that are sent to you will be made exclusively in a

electronically, through the Unique Authorized Electronic Address (dehu.redsara.es) and the

Electronic Notification Service (notifications.060.es), and that, if you do not access

their rejection will be recorded in the file, considering the process completed and

following the procedure. You are informed that you can identify before this Agency

an email address to receive the notice of making available to the

notifications and that failure to practice this notice will not prevent the notification

be considered fully valid.

Finally, it is noted that in accordance with the provisions of article 112.1 of the

LPACAP, there is no administrative appeal against this act.

Mar Spain Marti

Director of the Spanish Data Protection Agency

935-080323

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

22/23

>>

SECOND: On April 13, 2023, the claimed party has proceeded to pay

the sanction in the amount of 18,000 euros making use of the two reductions

provided for in the initiation Agreement transcribed above, which implies the

recognition of responsibility.

THIRD: The payment made, within the period granted to formulate allegations to

the opening of the procedure, entails the waiver of any action or appeal via

against the sanction and acknowledgment of responsibility in relation to

the facts referred to in the Commencement Agreement.

FUNDAMENTALS OF LAW

Yo

Competence

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

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

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

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

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

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

of data.

Likewise, article 63.2 of the LOPDGDD determines that: "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

Termination of the procedure

Article 85 of Law 39/2015, of October 1, on Administrative Procedure

Common for Public Administrations (hereinafter, LPACAP), under the heading

"Termination in disciplinary proceedings" provides the following:

"1. Initiated a disciplinary procedure, if the offender acknowledges his responsibility,

The procedure may be resolved with the imposition of the appropriate sanction.

2. When the sanction has only a pecuniary nature or it is possible to impose a

pecuniary sanction and another of a non-pecuniary nature but the

inadmissibility of the second, the voluntary payment by the presumed perpetrator, in

any moment prior to the resolution, will imply the termination of the procedure,

except in relation to the replacement of the altered situation or the determination of the

compensation for damages caused by the commission of the offence.

3. In both cases, when the sanction is solely pecuniary in nature, the

The competent body to resolve the procedure will apply reductions of at least

20% of the amount of the proposed penalty, these being cumulative among themselves.

The aforementioned reductions must be determined in the notification of initiation

of the procedure and its effectiveness will be conditioned to the withdrawal or resignation of

any administrative action or resource against the sanction.

The percentage reduction provided for in this section may be increased

according to regulations."

According to what has been stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: DECLARE the termination of procedure EXP202201318, in

in accordance with the provisions of article 85 of the LPACAP.

SECOND: NOTIFY this resolution to BARNA PORTERS SEGURETAT,

S.L.

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 as prescribed by

the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations, interested parties may file an appeal

administrative litigation before the Administrative Litigation 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.

Mar Spain Marti

Director of the Spanish Data Protection Agency

936-040822

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es