 Procedure No.: PS/00461/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

FACTS

FIRST: The inspection actions are initiated by the receipt of a letter of

notification of security breach of personal data sent by CAIXABANK,

S.A. in which they inform the Spanish Data Protection Agency (AEPD) that,

On September 2, 2019, the business unit involved began to

detect abnormal behavior in the client portfolio of certain former employees,

verifying possible leaks of information by them, before resolving their

contracts with the entity.

Reason for late notification:

They state that since the incident was reported, different investigations have been carried out.

internal actions aimed at verifying that the breach had actually been closed

produced, and its scope. It is when the actions to be carried out have been specified and defined.

carry out, including reporting the breach to the AEPD.

SECOND: In view of the aforementioned data security breach notification

data, the Subdirectorate General for Data Inspection proceeded to carry out

of previous investigation actions, having knowledge of the following

ends:

BACKGROUND

Date of notification of the security breach of personal data: January 17,

2020.

INVESTIGATED ENTITY

CAIXABANK, S.A. with NIF A08663619 and with address at c/ Pintor Sorolla nº2-

4,46002, Valencia.

RESULT OF THE INVESTIGATION ACTIONS

On May 5, 2020, information was requested from CAIXABANK, S.A. and of the

The response received shows the following:

Regarding the chronology of events.

At the beginning of September 2019, the Entity's private banking business unit

detected abnormal behavior in the client portfolio of two former employees.

Former A.A.A. and B.B.B. performed managerial functions advising

clients in relation to the management of their financial assets to conserve and

optimize your performance; and as such had access to sensitive personal information

and sensible of such clients.

Having noticed indications of a possible illegal disclosure to third parties of data

personal data, the Entity's Internal Audit area carried out an analysis that

culminated with the issuance on October 28, 2019 of Audit Report no.

BEXXX, of which they provide the part that they understand to be sufficient for the purposes of the report of the

personal data security breach. The Entity detected that both

former employees, before leaving as employees, on July 29, 2019,

had seized and disclosed to third parties outside the entity information

staff:

A.A.A. revealed to third parties, without authorization, confidential information of 187 clients, which

leaked through various emails. As confirmed in the report of

audit, on July 24, 2019, 6 emails were sent, and on July 29

of 2019, 19 emails were sent. The emails were

sent by A.A.A. to your home email address and another email address

external email from a third party. The data subject to dissemination included the DNI of

clients, information on positions, returns and equity variations

annual.

B.B.B., leaked confidential information to third parties of 32 clients between June 20

and on July 28, 2019, using 18 emails. Among the data subject to

diffusion included the DNI of clients, returns and changes in equity

annual, as well as tax documentation.

On October 4, 2019, the Entity requested through burofax to the

former employees, warning them of the illicit nature of their conduct, requesting that they

refrain from using and disclosing the stolen data.

On October 8, 2019, the Entity sent a burofax to

BANKINTER, S.A. (where former CaixaBank employees worked) of which

provide a copy, warning of the actions carried out by A.A.A. and B.B.B. with the final purpose

that the Entity adopt the necessary preventive measures in relation to the

personal data of CaixaBank customers.

On January 17, 2020, the AEPD was notified of the security breach.

On January 24, 2020, the Entity filed a complaint with the courts of

instruction of Madrid, given that such facts could constitute a crime at

affect the fundamental right to customer privacy, banking secrecy and

protection of trade secrets.

On February 14, 2020, after having filed the aforementioned complaint, it was

made additional notification to the AEPD, informing of the new measures adopted

in this regard by CaixaBank.

On February 4, in order to preserve the confidentiality of the data

obtained irregularly by former employees, an agreement was reached to

confidentiality and non-competition. By virtue of said agreements, Messrs. A.A.A. Y

B.B.B., undertook to keep the secret and maintain the confidentiality of the

information obtained irregularly and, in general, of all sensitive information

and confidential to which they had access during the term of their employment relationship as

employees of the Entity, undertaking not to reproduce, publish, distribute or

communicate it to third parties. Likewise, they were forced to immediately destroy all the

information, in all media, commitment expressed with the signing of the Certificate

of Destruction that accompanies each of the agreements.

On March 19, 2020, the AEPD was informed of the closure of the

security.

Measures to minimize the impact of the gap.

Sending burofax to former employees requesting the destruction of the information.

Sending of burofax to BANKINTER warning of the facts and requesting that they not

use of information.

Presentation of the complaint.

Adoption of the confidentiality agreement and certificate of destruction of the

information.

Regarding the affected data.

The number of those affected by the breach was a total of 219. The information that was seen affected was: DNI, economic-financial information, position information, returns and annual changes in equity.

The possible consequences for those affected are the disclosure to third parties of their personal information. In the agreements and certificates of destruction of the information, it is collected that all copies of emails that contained personal data of the entity's clients were destroyed.

From the investigations carried out, it is not concluded that the personal data disclosed have been used by third parties.

The Entity has concluded that the communication to those affected was not appropriate, taking into account note that appropriate measures have been taken to prevent the violation of security has implication in the rights and freedoms of the affected clients.

Regarding the actions taken for the final resolution of the breach.

To resolve the gap, an agreement was reached with the former employees with the objective of maintaining the confidentiality of the information of the affected clients.

The agreement includes obligations to destroy the information and confidentiality. Compliance with the agreement was ratified by employees by issuing and signing a certificate of destruction of information.

Regarding the security measures implemented before the breach.

They provide a copy of the Record of Treatment Activities of the Private Banking area and Premier Banking, area to which the employees belonged.

The data processing activities that were compromised were carried out
carried out prior to the entry into force of the General Regulation for the Protection of
Data and have not undergone any modification for what they consider was not
neither a risk analysis nor an impact assessment is necessary.
Employees are subject to compliance with the Code of Ethics that in its section
seventh includes the obligation of confidentiality. They are also required to
compliance with internal rule number 137, which refers to the Code of Ethics, of the
which provide a copy. Specifically, point 2.1 of rule 137 establishes the
principles that should govern the activity of people subject to the code of ethics, among
them "The confidentiality of the information that is treated, which is constituted as a pillar
foundation on which the relationship of trust with the groups with which the
that employees interact.
The internal regulations of the Entity include the preservation of the privacy of the
customers as a fundamental pillar of the activity carried out by employees and is of
mandatory compliance and knowledge for all of them. Additionally, they are made
periodic training that must necessarily be passed by employees, because they are
linked to their variable remuneration.
At the moment in which an employee initiates a query through the Terminal
Financial, two notices appear. The first notice reminds the employee that in order to
consult clients not related to the office to which it belongs, there must be a
justifying cause. Specifically, the employee must select one of the
following three options (i) the client is present and has expressly requested the
query, (ii) the client is not present but the query is related to a
professional reason and (iii) the consultation is necessary for the provision of
Public Administrations, judges or Courts.

Once the employee selects which of the three reasons enables him to consult the customer data, another control appears indicating that the query requires confirmation. It is recalled that the consultation will be monitored for its treatment as possible breach of the General Data Protection Regulation and the employee You must confirm that you want to continue with the query.

Regarding the measures implemented after the gap.

In response to the security breach that occurred, the process has been initiated to carry out the corresponding impact assessment.

THIRD: On January 4, 2021, the Director of the Spanish Agency for Data Protection agrees to initiate sanctioning proceedings against CAIXABANK, S.A. for the alleged infringement of article 33 of the RGPD, typified in accordance with the provisions in article 83.4 of the aforementioned RGPD, qualified as slight for the purposes of prescription in Article 74.m) of the LOPDGDD.

FOURTH: On January 21, 2021, the respondent presents allegations to the initial agreement, in which, in summary, it states that the notification of the breach of security to the AEPD was carried out at the moment in which it was noticed that it was probable that it constitutes a risk to the rights and freedoms of individuals affected and requests the annulment of the initial agreement due to lack of concurrence of the infringement provided for in article 33 of the RGPD.

PROVEN FACTS

FIRST: At the beginning of September 2019, the private banking business unit of the Entity begins to detect anomalous behavior in the client portfolio of

certain former employees, verifying possible leaks of information by them.

SECOND: The Entity's Internal Audit area carries out an analysis that

culminates with the issuance, on October 28, 2019, of Audit Report no.

BEXXX, by which it is detected that two employees had obtained information

sensitive and confidential in an irregular manner.

THIRD: On January 17, 2020, CAIXABANK, S.A. notifies the AEPD of the

security breach.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of

control, and as established in arts. 47 and 48.1 of the LOPDGDD, the Director of

The Spanish Agency for Data Protection is competent to resolve this

process.

II

Article 89.1.d) of Law 39/2015, of October 1, on Administrative Procedure

Common to Public Administrations (LPACAP) states the following:

“Article 89. Proposed resolution in sanctioning procedures.

1. The investigating body will resolve the completion of the procedure, with a file of the

actions, without it being necessary to formulate the resolution proposal,

when in the procedure instruction it becomes clear that there is any

of the following circumstances:

a) The non-existence of the facts that could constitute the infraction.

b) When the facts are not accredited.

c) When the proven facts do not constitute, in a manifest way, an infringement

administrative.

d) When it does not exist or it has not been possible to identify the person or persons

liable or appear exempt from liability.

e) When it is concluded, at any time, that the infraction has prescribed."

Article 28.1 of Law 40/2015, of October 1, on the Legal Regime of the Sector

Public (hereinafter LRJSP) states the following:

Article 28. Responsibility.

"1. They may only be sanctioned for acts constituting an administrative infraction.

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

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

independent or autonomous estates, which are responsible for them

title of fraud or guilt."

Article 70 of Organic Law 3/2018, of December 5, on Data Protection

Personal and Guarantee of Digital Rights, states the following:

Article 70. Responsible subjects.

"1. They are subject to the sanctioning regime established in Regulation (EU) 2016/679

and in this organic law:

a) Those responsible for the treatments.

b) Those in charge of the treatments.

c) The representatives of those responsible or in charge of the treatments do not

established in the territory of the European Union.

d) Certification entities.

e) The accredited entities for the supervision of codes of conduct.

2. The sanctioning regime will not apply to the data protection delegate

established in this Title."

In accordance with the foregoing and in view of the arguments presented, in the sense

that the notification of the security breach to the AEPD was made at the time

in which it was warned that it was likely to constitute a risk to

rights and freedoms of people, it must be accepted and proceed to

file of the sanctioning procedure, since the analysis of the entity for the

decision making related to the notification of security breaches to the

control authority, is carried out in accordance with the provisions of the Guide for the management and

notification of security breaches based on the parameters that in the same

They indicated. In addition, it should be noted that the investigated entity had implemented

security measures that, in principle, were adequate to guarantee that the

personal data were not accessible by third parties and, as evidenced by the facts, in

as soon as the attack was detected and confirmed by the entity, they were adopted in a

immediately a series of additional security measures in order to minimize the

risks and extreme difficulties in accessing and extracting information.

Therefore, in accordance with the applicable legislation, the Director of the Agency

Spanish Data Protection RESOLVES:

FIRST: FILE this sanctioning procedure.

SECOND: NOTIFY this resolution to CAIXABANK, S.A. with NIF

A08663619 and with address at c/ Pintor Sorolla nº2-4,46002, Valencia.

Against this resolution, which puts an end to the administrative procedure 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 reconsideration before the Director of the Spanish Agency for Data Protection within a month from counting 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 in article 46.1 of the aforementioned Law.

Finally, it is pointed out 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 by

writing addressed to the Spanish Agency for Data Protection, presenting it through Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other registers 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 within a period of two months from the day following the

notification of this resolution would end the precautionary suspension.

938-131120

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es