 Procedure No.: PS/00179/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: On 02/04/2019, the Director of the Spanish Agency for

Data Protection agrees to initiate investigative actions in relation to the

notification of a security breach made by AIR EUROPA LÍNEAS AÉREAS,

S.A., with CIF ***CIF.1 (hereinafter AIR EUROPA), relating to unauthorized access

to contact information and bank cards that affects 489,000 interested parties and

a volume of 1,500,000 records.

However, on 02/28/2020, it was agreed to open new actions of

investigation to AIR EUROPA and incorporate to these the documentation that integrated the

previous actions of file E/02564/2019, which were declared expired.

The security breach notification was made on 11/28/2018 and 01/22/2019

as initial and complete notification.

Subsequently, on 01/22/2019 another notification is made to correct information

provided, according to AIR EUROPA, to discrepancies between the acknowledgment of receipt

issued by the electronic headquarters of this Agency and the data actually entered

in the online form. The three notifications contain, among others, the following

information:

 That on 11/27/2018 there were repeated attempts to notify the

to this Agency through the form provided for this purpose at the headquarters

electronically but the online notification procedure made it impossible to

presentation by said means, proceeding to the presentation in a

initial and face-to-face on 11/28/2018.

 Data controller: AIR EUROPA whose data has been included in the

Investigated Entities section.

Date of detection of the breach: ***DATE.1

 Means of detecting the breach: AIR EUROPA receives a notification by

part of Banco Popular regarding a potential security incident, which

determines the activation of the incident response plan by AIR

EUROPE, on 10/17/2018.

Breach start date: 05/12/2018

 Gap resolved as of 11/17/2018.

 Summary of the incident: the security incident has led to unauthorized access

authorized to bank card information, numbering, date of

Reason for late notification: N/A

expiration and CVV that could have been used for the commission of

fraudulent operations. Although all those identified were canceled

before it is established that any damage has been caused to the

interested.

In some cases (approximately 2,500) the identity of the holders of the

bank cards has also been compromised.

 Typology: Confidentiality breach (unauthorized access).

 Means by which the breach has materialized: Hacking and malware.

 Context: External (purposeful action)

 That before the breach the following preventive measures were applied:

Network security:

Own human team with more than 10 years of experience in management and network administration, LAN and WAN.

The company has designed and provided training to employees on the use of the tools made available to them in accordance with current legislation.

AIR EUROPA uses 1.-[……].

Periodically (XXX) an evaluation program of vulnerabilities to monitor potential security breaches in known vulnerabilities.

In addition to the firewall systems that allow managing and blocking unauthorized access, there is a 2.-[……].

To protect the user's browsing, there is a 3.-[……].

Information protection and access controls:

Access to information systems requires the identification and authentication of all users 4.-[……] (XX).

XX is connected to system 5.-[……].

There is a password renewal policy by which they are forced to change the same every XXX.

The policy of 6.-[……].

Application access permission management policies 7.-[……] allowing the principle of least privilege to be applied.

Prevention:

A few months ago, AIR EUROPA began a process aimed at drawing up a

Security Master Plan in order to have a broader scenario of

threats and define a more effective strategy. 8.-[……].

 That the categories of data affected are basic data and information about

bank cards such as number, expiration date and CVV.

 That there are no special categories of affected data.

 That the approximate number of affected data records is 1,500,000

 That the profile of the affected subjects are clients, being the number

Approximate number of people affected 489,000.

 That the nature of the potential impact on the subjects is fraud.

 That the possible consequences is disclosure to third parties/dissemination in

internet and that the data can be exploited for other purposes.

 That classifies the severity of the consequences as “Medium”.

 That the measures taken to solve the breach and minimize the impact were:

o Carrying out a preliminary investigation.

o Hiring a forensic company ***COMPANY.1 for the

provision of support and assistance in the analysis of the incident.

o Recruitment of a company specialized in analysis and resolution of

Incidents *** COMPANY.2.

o Follow-up of tasks and planning of improvements and actions to be implemented

in the systems in order to "close doors" and reduce the risk.

o Review of all the security measures and reinforcement of the

themselves.

o Chronology of the actions followed described in documents

attachments.

 That the interested parties will not be informed for the following reasons:

o There is only a record of 11 requests for information by

part of clients in relation to this event and is responding to

all of them. The existence of other affected is unknown.

o That the technical protection measures have been adopted and

appropriate organizational arrangements that ensure that there is no longer

probability that any risk to the rights and

freedoms of the data subjects affected by the security breach.

o That they understand that at this time it is more burdensome for

general interests and those of the interested parties make a communication

public since they do not have contact information for all the

affected people.

 Attached documents are provided that contain, among others, the following

manifestations:

o That immediately after learning of the breach, a

the company specialized in security breaches and forensic analysis and

***COMPANY.3.

o The company ***EMPRESA.2 was hired for the purpose of analyzing the

scope, together with ***EMPRESA.3, and apply the measures

necessary to correct the incident.

o That the scope of the breach is not yet fully known.

The security incident has led to unauthorized access. I know

makes this notification in a preliminary way to provide the

information available so far.

o That a series of measures of a technical nature were adopted that

carried out by putting the focus first on activities of

containment and then in preventive activities.

o That after having analyzed the information that AIR EUROPA believes

having been compromised, it is highly unlikely that only

Spanish stakeholders have been affected. However, AIR

EUROPE is not currently in a position to identify the

specific nationalities of all affected stakeholders.

o Chronology of the actions followed:

□

□

□

□

□

□

□

□

□

***DATE.1. AIR EUROPA receives a notification from
VISA (Banco Popular) regarding a potential incident of
security which determines the activation of the Response Plan
to Incidents (PRI) on October 17, 2018.
10/18/2018. As part of the PRI, the company is contacted
***COMPANY.3 for the provision of support and help in the
forensic analysis of the incident whose hiring took place on 22
October 2018.
10/24/2018 to 10/31/2018. Collection of evidence and information
necessary.
11/05/2018 to 11/08/2018. Analysis of the information collected. The
On 11/8, the forensic analyst confirmed the existence of a
gap.
08/11/2018. ***EMPRESA.2 is contacted with the aim of
strengthen internal security teams and work
jointly with ***COMPANY.3.
09/11/2018. Work begins on ***COMPANY.2 to go
"closing doors" and progressively reduce the risk.
11/14/2018. The review tasks of the set of
security measures and, as appropriate, reinforce them.
On behalf of ***EMPRESA.2 and the forensic team identifies
that from a server you are contacting an IP not
recognized.
11/15/2018. AIR EUROPA receives specific instructions from
the forensic team with 8 measures aimed at containing the

issue. With the support of the ***EMPRESA.2 team, it is assigned

highest priority to containment tasks.

11/17/2018. Confirmation by ***COMPANY.2 and

***COMPANY.3 that the breach is contained.

11/23/2018. It is confirmed by ***COMPANY.2

the

carrying out 90% of the containment and protection actions and

that the pending tasks are to be completed in the next

days. The effectiveness of the measures of

real-time monitoring that continue to be deployed to

guarantee the detection of any intrusion.

SECOND: the General Subdirectorate of Data Inspection proceeded to carry out the

following actions:

On 04/01/2019, AIR EUROPA sends this Agency the following information and

manifestations:

1. An audit report carried out by ***COMPANY.4 and dated to

12/20/2018 with the following manifestations:

The "Incident Background" section states:

“In October 2018, GLOBALIA was informed by the companies of

credit cards that a large number of credit cards,

some 4,000 had been used to commit fraud. The data

stolen included personal and financial data of the clients of

GLOBALIA who made reservations and modifications on AirEuropa.com.

The data did not include travel or passport data.”

Manifestations in the rest of the audit document:

a.

b.

c.

d.

and.

F.

g.

h.

Yo.

“The first confirmed access to the GLOBALIA network by the

attacker took place through on May 12, 2018.”

“Following this initial access, the attacker compromised a series of

GLOBALIA and IRIS systems consider that the attacker followed

accessing the systems and accounts of GLOBALIA at least until the

August 11, 2018.”

“Although IRIS has not been able to confirm how the attacker managed to exfiltrate

information from the GLOBALIA network or what was exfiltrated, taking into account

of the limitation of records, what IRIS has confirmed is that the

attacker had collected at least 488847 unique credit cards”

“Based on the sample of 4,939 unique credit cards already declared

fraudulent, 1185 were found in the collection above

mentioned."

“The attacker viewed and filed in ***FILE.1 at least 2651

unique card numbers, CVVs, expiration dates and names of

Cardholder."

“In total the attacker compromised at least 12 systems and a minimum

of 2 service accounts in support of your operation”

“For the initial access, the attacker took advantage of 9.-[…….] to

get access to the network for the first time”

“Any system exposed to the Internet, 10.-[……].”

“Furthermore, subsequent investigations of the accounts

compromised by the attacker, such as the service account

GLOBALIA\EJP, revealed that it used a password that did not meet the

complexity and length requirements in line with best practice of the

sector, which would have made it easier for the attacker to

compromise this account.”

“Although IRIS was unable to confirm the data regarding how the

attacker exfiltrated information due to record limitation, some

research data indicate the time when they could be taken

the data and from where. Given that most of the data

sensitive data that were collected by the attacker was found or

transferred to the server ***FILE.1, and that the server also

had the only viable mechanism of persistence, it is likely

that the attacker used ***FILE.1 as a test server from

which to exfiltrate information. Similarly, a statistical analysis of

the firewall logs revealed that the largest number of connections

to the IP address controlled by the attacker, ***IP.1, from the systems

of GLOBALIA, took place between May 14 and June 4, with a

peak from May 19 to 21, indicating that the attacker got down

to the work Given the volume of activity, it is possible that he also had

data exfiltration takes place during these time frames,

although the fact that the attacker accessed specific files

related to credit cards later, in June, could

indicate that the exfiltration also took place later in the

same month.”

“To maintain access to the network, the attacker used tools

publicly available, from 11.-[……] in the systems that are

communicated with the IP address controlled by the attacker ***IP.1.”

“No further malicious activity was observed regarding the same attacker or

threat actor after August 11, 2018”

J.

k.

l.

m. “The IP address controlled by the attacker was blocked on the 15th of

n.

a.

november."

“Irregular registry settings were observed on systems

analyzed, so that only some systems stored

locally archived log files; for example, the scripts

executed by Powershell were only logged in some

systems.

Audit logs are important during a security incident.

security to reconstruct the activities of the attacker…

Therefore, it is recommended to review the current audit policy and

retention and apply it evenly throughout the environment. If not used

already, it is also recommended to assess the possibility of centralizing the

collection of logs on a dedicated platform, such as a

Security Information and Incident Management (SIEM) product,

…"

"Although it has not been possible to determine the exact source of the

infection of the systems in scope, one of the most

probable is that 12.-[……]."

b.

a.

"Block and monitor outbound traffic to external IP addresses

suspicious behavior is a good way to detect behavior

abnormal originating from the network.

In this incident we have 13.- [……], communicate with IP addresses

external that were not related to any payment system,

nor were they justified by other business needs.”

“During the investigation, IRIS observed various systems with

operation longer than one year, so that the systems

operatives did not have patches for such a long period.”

2. A calendar of technical tasks undertaken for the closure of the

gap and the protection improvements implemented that it has had in

consideration, as stated by AIR EUROPA, the measures and

recommendations issued by ***COMPANY.2 after analyzing the incident of

security. This calendar contains tasks between 11/14/2018 and

on 02/13/2019 and are classified into the following groups:

a. XXX XXX update.

b. Restrict firewall rules.

c. Blocking and registration of ***IP.2.

d. Cleanup of local users XXX XXX.

and. Password changes.

 14.- [……].

F. virus.

g. Application 15.-[……].

h. Patching of vulnerabilities and update of involved servers

in the incident.

Installation XXX XXX.

Yo.

J. 16.-[……].

k. Replatformed from XXX XXX.

l. Configuration 17.-[……].

3. AIR EUROPA states that it has received only 20 communications from

clients due, for the most part, to inconveniences derived from the cancellation

of the card by your bank, without showing any type of damage

suffered, and through which they request more information. That

only 3 of them stated that they had suffered some type of injury

economic result of the use, by third parties, of personal data

obtained through the attack. AIR EUROPA has responded

attending to the information requirements requested by the interested parties.

4. Provides risk analysis regarding security measures in the

processing of online sales data to passengers of AIR EUROPA which

It consists of a one-page document that analyzes 9 risks.

5. Provides risk analysis carried out regarding the need or not of

notification to this Agency and to the interested parties. This analysis shows:

a. The art. 34.3 of the GDPR establishes three exceptions to the obligation to

notify interested parties:

 Regarding 34.3.a):

“In relation to the AIR EUROPA systems, there were no

specific measures, 18.-[……]. However, the information

accessed by the attackers does not include information

sensitive as special categories of personal data,

postal addresses or telephone numbers,

passport or ID or date of birth. This information

sensitive is not stored together with card information

banks as a security measure. As a result, it is very

difficult to identify unique individuals within the data set."

 Regarding 34.3.b):

"…once the incident has been identified by the banking entities,

these and the issuers of the compromised bank cards

they proceeded to block and report said block to the

interested parties so that the compromised data remains

unusable…"

A communication model made by the entity is provided

Bankinter to its customers.

 Regarding 34.3.c):

"…it is virtually impossible to uniquely identify

stakeholders from this data set, as there is no

has their contact details.

Therefore, if it is determined that a notification must be made

interested parties, AIR EUROPA would have to carry out a

public communication instead of individual notifications.

From AIR EUROPA it is understood that at this time it is

more burdensome for the general interests and those of the

stakeholders make a public communication, as there is no

no benefit derived from that communication."

b. That, according to the analysis methodology of the AEPD, the result

quantity would not exceed the threshold established for such notification

(30 vs 40) while the qualitative threshold would be exceeded. Without

However, and taking into account the foregoing, AIR EUROPA has decided not to

notify the interested parties arguing that the incident is not

likely to pose a high risk to the rights and freedoms of

the same.

c. That in those cases in which a high risk could be observed

one or more exceptions from those listed in art. 3. 4

GDPR. In this sense, the provisions of art. 34.3 a) and b).

On 11/14/2019, AIR EUROPA sends this Agency the following information and

manifestations:

1. That 100% of the share capital of AIR EUROPA belongs to GLOBALIA

BUSINESS CORPORATION, S.A. That at AIR EUROPA there is a team

responsible for information systems headed by the figure of the CIO.

At the operational level, the functions related to the provision of

infrastructure and administration of information systems and

communications are provided by

GLOBALIA SYSTEMS AND

COMUNICACIONES S.L.U., a company that belongs 100% to GLOBALIA

BUSINESS CORPORATION, S.A.

2. Provide a signed copy of the assistance and management contract in the systems area

of information and communications dated 10/31/2009 between AIR EUROPA

AIRLINES, S.A.U. and GLOBALIA SYSTEMS AND COMMUNICATIONS,

S.L.U. where it is manifested, among others:

a. That GLOBALIA SISTEMAS will assist AIR EUROPA in the areas of

information and telecommunications systems.

b. That the service to be provided by GLOBALIA SISTEMAS will have a

integral, in a way that allows AIR EUROPA the total outsourcing of

services in the areas of information systems and

communications.

c. That GLOBALIA SISTEMAS will carry out, on its own initiative, the

and appropriate tasks for the development of the benefits previously

identified. Notwithstanding the foregoing, GLOBALIA SISTEMAS will submit

to the approval of AIR EUROPA the projects to be developed and will pay

accounts of the negotiations in the course of organized meetings, of

mutual agreement, with a frequency not exceeding quarterly.

3. Provides a signed copy of the novation of the data processing manager contract

personal data dated 10/31/2019, according to which, GLOBALIA SISTEMAS

AND COMMUNICATIONS, S.L.U. is in charge of the treatment and AIR EUROPA

AIRLINES, S.A.U. is the data controller.

4. Provide a copy of the Cybersecurity Incident Response Plan of

GLOBALIA with an effective date of 07/05/2019 in its first version

as indicated by the version control of the document and the cover page of the document.

5. That the forensic report of ***COMPANY.3 is a report that is required by

rules banks on behalf of payment institutions that are members of the

PCI Council (as would be the case of VISA) to entities affected by a

incident, in order to evaluate the 19.-[……].

6. That the forensic report of ***EMPRESA.3 has a very specific purpose and

is oriented within the framework of identifying the volume of cards identified

as committed, which generally determines the compensation

that the PCI Council may require from the entity affected by the

incident.

Provides forensic report of ***EMPRESA.3 dated January 2019 and based on

in the investigation initiated on 10/25/2018 which contains the following

manifestations, among others:

a.

b.

c.

d.

“The investigation carried out by ***EMPRESA.3 identified evidence

conclusive of violation in AIR EUROPA”

“The investigation of ***EMPRESA.3 identified more than 2.7 million

unique card numbers that had been extracted from card systems

databases by the attacker. Although some of the data from the

cards were 20.-[……], the attacker managed to use

21.-[……] tools to obtain clear text data.”

“The intrusion probably originated from insecure systems

available through the internet. ***COMPANY.3 identified several

devices that had not been regularly patched…”

“Summary of possible causes and list of attack vectors:

22.-[……]

b.

c.

a. There is evidence of violation of the data environment of the holders of the

cards.

“The attack began when the attacker accessed XXX XXX from a

server not properly segmented at XXX XXX”.

“The attacker had a systematic connection to an external host. 23.-,

***COMPANY.3 [……]. However, he did visualize how the attacker

created several files and later compressed them into a single

File, Archive. 24.-[……].”

d. Possible exposure of data types, among others; owner's name

card, cardholder address, expiration date.

and. That the total number of exposed cards is 2722692, not being that

the number of cards that are at risk.

2. That, in relation to the reason for not detecting the breach until

***DATE.1 despite the fact that the attack began on 05/12/2018, AIR EUROPA

states that the breach occurred as a result of an APT, an attack

directed and sophisticated, planned and executed in a professional and

treacherous

Likewise, it states that:

“the attack suffered by the Society is a type of “attack […] designed to

endure over time and manage to evade all the security measures of the

most common platforms” as described by INCIBE in an article

published on its website on June 16, 2016 and signed by A.A.A.. It is,

therefore, a type of stealthy attack whose ultimate goal is to filter

sensitive information of an organization and erase the traces upon completion,

which makes them extremely difficult to detect”

1. States that the key dates of the drafting of the Master Plan

of Security (PDS) are:

a. July 2019: definition of the preliminary scope of business services

that will be evaluated for the development of the PDS.

b. September 11, 2019: launch meeting.

c. January 31, 2019: project closure.

d. February 3, 2020: entry into force of the PDS.

2. Provides a document entitled "Procedure for critical updates and

security” and states that this procedure has been applied in a

usual since before the incident.

a. This document states 25.-[……].

“26.-[……]”

b. In this document it is stated in section 27.-[……].

c. In this document it is manifested in 28.-[……].”

3. Provides the AIR EUROPA Information Security Manual dated

of last modification of the document on 10/31/2013 being the object of this

document respond to the obligation established in article 9 of the Law

Organic 15/1999.

4. States that “it is relevant to state, as important data for purposes

to ratify the non-existence of relevant effective damages, that the number of

complaints received from users of the Company that could

be related to the incident has been very small (2 claims in

total without request for compensation). This confirms the analysis that the

attackers have not been able to obtain sensitive or relevant information and that, with

the information that could have been stolen, the existence of numerous

technical and organizational security measures throughout the process chain

(including entities involved in payment services) has made

that information cannot have been used to cause serious harm."

On 06/04/2020, AIR EUROPA sends the impact assessment to this Agency

of the treatment of "Sales to customers through alternative channels".

THIRD: On 06/23/2020, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, in accordance with the

provided in articles 63 and 64 of Law 39/2015, of October 1, of the

Common Administrative Procedure of Public Administrations (hereinafter,

LPACAP), for the alleged infringement of articles 32.1 and 33 of the RGPD, typified

in accordance with the provisions of article 83.4.a) of the aforementioned RGPD.

FOURTH: Once the aforementioned initiation agreement was notified, the respondent filed with the AEPD

requesting a copy of the file and extension of the term granted for the

presentation of arguments, which was granted in five more days.

On 07/16/2020, the respondent submitted a brief of allegations in which, in summary,

stated that it was not true that the security breach had not been reported

but once there were well-founded indications that the cyberattack suffered had

affected a considerable number of data was notified; that he

claimed at all times has responded to the requirements formulated by the

AEPD; the inadmissibility of the infringement of article 33 of the RGPD since the

notification was made; the lack of motivation and responsibility appreciated by the

AEPD; that in the resolutions issued by the AEPD regarding security breaches

less sophisticated than the one analyzed, most of them were always archived

that technical security measures be accredited prior to the incident and

they adopted palliative measures subsequently, as occurs in the instant case; its

disagreement with the graduation of the sanction in the event of a possible violation of article

32.1 of the RGPD due to the non-concurrence of aggravating circumstances and the existence of mitigating factors that

have not been considered in the startup agreement.

FIFTH: On 11/23/2020, the instructor of the procedure agreed to open

a period of practice of tests, practicing the following:

Consider reproduced for evidentiary purposes all the documents obtained and

generated by the Inspection Services and the Report of previous actions of

Inspection that are part of file E/01909/2020.

Consider reproduced for evidentiary purposes, the allegations to the initial agreement

PS/00179/2020 presented by the respondent and the documentation that they

accompanies.

Request the respondent in reference to a date prior to the start of the gap

produced:

- Description (including the name of the servers and databases

included in them) the different system environments from the point of view of

security, where they store customer data and their bank cards,

including at least the data of postal address, telephone numbers,

passport numbers, DNI, date of birth, name of the holder of the

card, card PAN, card expiration date and your CVV code.

Likewise, indication of the types of data that are stored within each

environment/server/database and provide documentation proving the

applied security measures aimed at isolating the different environments

each.

- For each of the environments, servers and databases identified in

the previous section, provide a screenshot where it is displayed, for 50

records, all data stored together with the explanation of its

meaning.

Taking into account the Risk Analysis document delivered to this

Agency with name “Documento_3__PIA_Venta_on_line.pdf”, and the measures

security applied before the beginning of the breach, contribution of the following

information and documentation in force on the date prior to the start of the gap:

• Reason why they were not included in the risk analysis 29.-[…….].

• Reason why they were not adopting 30.-[…….]:

31.-[…….].

32.-[…….]

On 12/02/2020, the respondent submitted to the AEPD a letter of extension of the

period granted for the provision of evidence that was granted in five days

plus.

On 12/16/2020, the respondent responded to the requested information, whose

content work in the file.

SIXTH: On 02/05/2021, a Resolution Proposal was issued in the sense that by

the Director of the Spanish Agency for Data Protection will be sanctioned

claimed, for infringement of articles 32.1 and 33 of the RGPD, typified in article

83.4 of the RGPD, with fines of €500,000 (five hundred thousand euros) and €100,000 (one hundred thousand euros), respectively.

On 02/10/2021, the respondent submitted to the AEPD a letter of extension of the term granted for the presentation of arguments, which was granted in two days plus.

On 02/25/2021, the respondent presented this brief in which he alleged in summary: the importance for the claimed person supposes both the incident produced and the protection of the personal data of all its clients; the helplessness caused by the lack of consideration of the evidence presented at the last request for information from the AEPD; the express challenge of the entire report of the Foregenix company; the inadmissibility of the sanction imposed for alleged infringement of article 33 of the RGPD and, subsidiarily, its prescription; disagreement with the imputation of infringement of article 32 of the RGPD in relation to the measures appropriate technical and organizational measures to guarantee a level of security adequate to the risk and inappropriateness of using forensic reports as evidence that Air Europe did not have adequate security measures; lack of proportionality in the analysis of the aggravating circumstances taken into account by the AEPD for the graduation of the sanction imposed as a consequence of the presumed infraction of the article 32.1 of the RGPD and the existence of mitigating circumstances that have not been considered when establishing the amount of the sanction and the disparity of criteria in relation to previous similar sanctioning procedures.

SEVENTH: Of the actions carried out in this procedure and of the

documentation in the file, the following have been accredited:

PROVEN FACTS

FIRST: On 11/29/2018, the AEPD receives a letter from the respondent stating that

on ***DATE.1 had received notification from Banco Popular regarding an incident of

security by triggering the incident response plan

10/17/1018.

SECOND: On 01/18/2019, the respondent provided complete notification through the

form enabled in the electronic headquarters of the AEPD, providing documents

annexes related to preventive measures applied prior to the incident;

Containment measures and additional information and Justification for not informing the

stakeholders affected by the incident.

THIRD: The person claimed on 04/01/2019 has provided: Forensic technical report

prepared by ***EMPRESA.2 in relation to the incident reported to the AEPD in

the one that analyzes the incidence produced and recommendations; noting that "In

October 2018, GLOBALIA was informed by credit card companies

credit that a large number of credit cards, some 4,000, had been

used to commit fraud. The stolen data included personal data and

financial statements of GLOBALIA customers who made reservations and changes in

AirEuropa.com. The data did not include travel or passport data" and that "The first

confirmed access to the GLOBALIA network by the attacker took place through

33.-[……] for an unknown account on May 12, 2018." Report

prepared by the technical team of the respondent which identifies the technical tasks

connections to close the gap and the protection improvements implemented,

following IBM recommendations; risk analysis regarding the measures

security in the processing of online sales data to Air Europa passengers;

the risk analysis carried out by the Company regarding the need or not to

notification to the AEPD and interested parties about the security breach

experienced.

FOURTH: The defendant on 11/14/2019 has provided a forensic report of

***COMPANY. January 3, 2019 based on research and analysis

of the possible causes, noting among others that "The investigation carried out by

***COMPANY.3 identified conclusive evidence of violation at AIR EUROPA"; copy

of the contract for assistance and management of information systems and communications of

10/31/2009 between GLOBALIA SISTEMAS Y COMUNICACIONES, S.L.U. and the claimed

in which they hold the status of responsible and in charge of the treatment

respectively; copy the Cybersecurity Incident Response Plan of

GLOBALIA of 07/05/2019 and Information Security Manual dated

10/31/2013

FIFTH: On 06/04/2020 the respondent provided an Impact Assessment of the

treatment of "Sales to customers through alternative channels".

SIXTH: The respondent has provided during the evidence period documents related to

measures it had in place prior to the declared security incident.

FOUNDATIONS OF LAW

Yo

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

control authority, and according to the provisions of articles 47 and 48 of the LOPDGDD,

The Director of the Spanish Agency for Data Protection is competent to initiate

and to solve this procedure.

II

Article 58 of the RGPD, Powers, states:

"two. Each supervisory authority will have all of the following powers

corrections listed below:

(…)

i) impose an administrative fine under article 83, in addition to or in

Instead of the measures mentioned in this section, according to the

circumstances of each particular case;

(…)”

The RGPD establishes in article 5 of the principles that must govern the

treatment of personal data and mentions among them that of "integrity and

confidentiality”.

The article notes that:

"1. The personal data will be:

(…)

f) treated in such a way as to ensure adequate security of the

personal data, including protection against unauthorized processing or

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

of appropriate technical or organizational measures ("integrity and

confidentiality")".

(…)

On the other hand, article 4 of the RGPD, Definitions, establishes in its sections

7, 8 and 12:

"(…)

7) "responsible for the treatment" or "responsible": the natural or legal person,

public authority, service or other body which, alone or jointly with others, determines the

purposes and means of treatment; whether the law of the Union or of the Member States

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

Specific criteria for their appointment may be established by Union Law.

or of the Member States;

8) "processor" or "processor": the natural or legal person,

public authority, service or other body that processes personal data on behalf of the

data controller;

(…)

12) "personal data security breach": any breach of the

security that causes the accidental or unlawful destruction, loss or alteration of

personal data transmitted, stored or otherwise processed, or the

unauthorized communication or access to said data;

(…)"

Likewise, article 24, Responsibility of the data controller,

establishes that:

"1. Taking into account the nature, scope, context and purposes of the

treatment as well as the risks of varying probability and severity for the rights

and freedoms of natural persons, the data controller will apply measures

appropriate technical and organizational measures in order to guarantee and be able to demonstrate that the

processing is in accordance with this Regulation. These measures will be reviewed and

will update when necessary.

2. When they are provided in relation to treatment activities,

The measures mentioned in paragraph 1 shall include the application, by the

responsible for the treatment, of the appropriate data protection policies.

3. Adherence to codes of conduct approved under article 40 or to a

certification mechanism approved under article 42 may be used

as elements to demonstrate compliance with the obligations by the

data controller".

And article 25, Data protection by design and by default, states that;

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

nature, scope, context and purposes of the treatment, as well as the risks of various

probability and seriousness that the treatment entails for the rights and freedoms of

natural persons, the data controller will apply, both at the time of

determine the means of treatment as at the time of the treatment itself,

appropriate technical and organizational measures, such as pseudonymisation, designed

to effectively apply the principles of data protection, such as the

minimization of data, and integrate the necessary guarantees in the treatment, in order to

comply with the requirements of this Regulation and protect the rights of

interested.

2. The data controller will apply the technical and organizational measures

with a view to guaranteeing that, by default, they are only processed

the personal data that is necessary for each of the specific purposes of the

treatment. This obligation will apply to the amount of personal data collected, to

the extension of its treatment, its conservation period and its accessibility. Such

measures shall in particular ensure that, by default, personal data is not

accessible, without the intervention of the person, to an indeterminate number of people

physical.

3. An approved certification mechanism may be used under the

Article 42 as an element that proves compliance with the obligations

established in sections 1 and 2 of this article".

Therefore, to correct a security violation, the person in charge of the

treatment must be able to recognize it and the consequence of such a violation is that the

data controller cannot guarantee compliance with the principles

regarding the processing of personal data, as established in article 5

of the GDPR.

The security of personal data is regulated in articles 32, 33 and

34 of the GDPR.

III

The GDPR defines security breaches of personal data as

those incidents that cause the accidental destruction, loss or alteration or

illicit personal data, as well as unauthorized communication or access to the

themselves.

Since last 05/25/2018, the obligation to notify the Agency of breaches

or security breaches that could affect personal data is applicable to

any controller of personal data processing, which underlines the

importance that all entities know how to manage them.

Consequently, as soon as the data controller has

knowledge that a data security breach has occurred

must, without undue delay and, if possible, no later than 72 hours

after you have become aware of it, notify the security breach of

personal data to the competent control authority, unless the

responsible can demonstrate, in accordance with the principle of proactive responsibility, the

Unlikely that the breach of the security of the personal data will entail a

risk to the rights and freedoms of natural persons.

The data controller must inform the interested party without delay

improper violation of the security of personal data in the event that it may

pose a high risk to your rights and freedoms, and allow you to take the

necessary precautions. The communication must describe the nature of the violation

of the security of personal data and the recommendations so that the person

affected physical condition mitigates the potential adverse effects resulting from the violation.

Said communications to the interested parties must be made as soon as possible.

reasonably possible and in close cooperation with the supervisory authority,

following its guidelines or those of other competent authorities, such as the

police authorities. Thus, for example, the need to mitigate a risk of damage and

immediate damages would justify a quick communication with the interested parties,

while it is possible to justify that the communication takes more time due to the need to

apply appropriate measures to prevent data security breaches

continuous personal or similar.

Article 33 of the RGPD establishes the way in which a notification must be made.

violation of the security of personal data to the control authority.

In this same sense, it is stated in Recitals 85 and 86 of the RGPD:

(85) If adequate measures are not taken in time, violations of the

security of personal data can lead to physical damage,

material or immaterial for natural persons, such as loss of control over their

personal data or restriction of their rights, discrimination, usurpation of

identity, financial loss, unauthorized reversal of pseudonymization, damage

for reputation, loss of confidentiality of data subject to professional secrecy,

or any other significant economic or social damage to the natural person in

question. Consequently, as soon as the data controller has

knowledge that a data security breach has occurred

personal data, the controller must, without undue delay and, if possible, no later than

72 hours after you have been aware of it, notify the violation of the

security of personal data to the competent control authority, unless

the person in charge can demonstrate, in accordance with the principle of proactive responsibility,

the improbability that the breach of the security of the personal data will entail

a risk to the rights and freedoms of natural persons. yes said

notification is not possible within 72 hours, it must be accompanied by a

indication of the reasons for the delay, information being able to be provided in phases without

more undue delay.

(86) The controller must notify the data subject without delay

improper violation of the security of personal data in the event that it may

pose a high risk to your rights and freedoms, and allow you to take the

necessary precautions. The communication must describe the nature of the violation

of the security of personal data and the recommendations so that the person

affected physical condition mitigates the potential adverse effects resulting from the violation.

Said communications to the interested parties must be made as soon as possible.

reasonably possible and in close cooperation with the supervisory authority,

following its guidelines or those of other competent authorities, such as the

police authorities. Thus, for example, the need to mitigate a risk of damage and

immediate damages would justify a quick communication with the interested parties,

while it is possible to justify that the communication takes more time due to the need to

apply appropriate measures to prevent data security breaches

continuing personal or similar.

IV

In the first place, the defendant is charged with the violation of article 32.1 of the

GDPR, which states:

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

nature, scope, context and purposes of the treatment, 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 measures and

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

which in your case includes, among others:

a) 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 evaluation of the effectiveness

technical and organizational measures to guarantee the security of the

treatment.

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

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

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

data transmitted, stored or otherwise processed, or the communication or

unauthorized access to said data.

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

certification mechanism approved under article 42 may serve as an element

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

present article.

4. The person in charge and the person in charge of the treatment will take measures to

ensure that any person acting under the authority of the controller or

of the person in charge and has access to personal data can only treat said

data following the instructions of the person in charge, unless it is obliged to do so

under the law of the Union or of the Member States".

Recital (83) states that:

"(83) In order to maintain security and prevent the treatment from violating the

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

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

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

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

regarding the risks and the nature of the personal data that must be

protect yourself. When assessing the risk in relation to data security,

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

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

transmitted, stored or otherwise processed, or the communication or access is not

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

Of the actions carried out and documentation provided to the file,

verified that the security measures that the investigated entity had in

relation to the data that it submitted to treatment, were not the most suitable for

guarantee the security and confidentiality of personal data at the time of

occurrence of the incident or bankruptcy.

As also points out in Recital 39:

“…Personal data must be processed in a way that guarantees a

adequate security and confidentiality of personal data, including for

prevent unauthorized access or use of such data and equipment used in the

treatment".

It should be noted that security measures are key when it comes to

guarantee the fundamental right to data protection since it is not possible

ensure the fundamental right to data protection if it is not possible to guarantee the

confidentiality, integrity and availability of personal data. For

To guarantee these three security factors, measures are necessary both of a nature technical as well as organizational.

Therefore, information security risk analyzes should focus on the ability to ensure confidentiality, integrity, availability treatment systems and services, as also contemplated by said Article.

One of the requirements established by the GDPR for controllers and data processors that carry out data processing activities personal information is the need to carry out a security risk analysis of information in order to establish security and control measures aimed at comply with the principles of protection by design and by default that guarantee the rights and freedoms of people.

It is necessary to point out that in the present case, in light of the reports ***COMPANY.3 accredited issued by companies serious vulnerabilities of the claimed systems, compromising the confidentiality and integrity of information security causing access unauthorized that led to and caused an illegal transmission of data.

***COMPANY.2 and

As stated in the ***EMPRESA.2 Report of 12/20/2018, “In October 2018, GLOBALIA was informed by credit card companies that a large number of credit cards, some 4,000, had been used to commit fraud. The stolen data included personal and financial data of the clients of GLOBALIA who made reservations and modifications on AirEuropa.com. data not included travel or passport data” that “The first confirmed access to the network of GLOBALIA by the attacker took place 34.-[……] for an account

unknown on May 12, 2018” and continues that after the initial access,

using 35.-[…….], the hacker compromised a series of GLOBALIA systems

continuing access until at least 08/11/2018; that it has been confirmed that

the attacker had collected 488847 unique credit cards; who committed to

least 12 systems and a minimum of 2 service accounts in support of your operation;

that all the system exposed to the Internet should have Authentication executed

multifactorial; that subsequent investigations of accounts compromised by the

attacker revealed 36.-[…….], which would have made the attacker find it more

easy to compromise this account; that the attacker likely used ***FILE.1

as a test server from which to exfiltrate information; than an analysis

statistical analysis of the firewall logs revealed that the greater number of connections

to the IP address controlled by the attacker, took place between May 14 and November 4.

June; that the attacker used publicly available tools, 37.-[…….] with the

IP address controlled by the attacker; that a log configuration was observed

irregular in the analyzed systems, so that only some systems

they stored locally archived log files.

The aforementioned company made a series of recommendations: review the policy

audit and retention and 38.-[…….]; Although it has not been possible to determine

exactly the source of the infection of the systems in scope, one of the hypotheses

most likely is 39.-[…….] observed different systems with a functioning

longer than one year, so 40.-[…….].

Likewise, the Report of ***EMPRESA.3, company contracted on 10/22/2018

by the claimed and specialized in security breaches and forensic analysis, from January

of 2019 states: that it had identified conclusive evidence of the violation of

security; the identification of 2.7 million cards that had been extracted from the

database systems by getting the attacker to use security tools

decryption present on systems; that access 41.-[…….]; a summary of the

possible causes that would have motivated the attack (42.-[…….]; the existence of

cardholder data environment breach evidence; that the attack

started when accessed 43.-[…….]; that the attacker had one with an external host and

that 44.-[…….]; the possible exposure of certain types of data (name of the

cardholder, cardholder address, expiration date).

Therefore, it follows from the foregoing that the security measures

technical and organizational measures implemented by the entity complained against were not appropriate

to guarantee a level of security appropriate to the risk and prevent unauthorized access.

authorized to customer data.

It should be noted that given the technological and digital evolution suffered by

personal data processing activities, they must be addressed from the point of

from the point of view of continuous risk management, defining from the design the measures

of control and security necessary for the treatment to occur respecting

the privacy requirements associated with the levels of risk to which they may be

exposed and periodically and continuously evaluating the effectiveness of the measures

of control implanted.

This also implies the protection of personal data from the design and

by default, that is, the controller must apply, both at the time of

establish the means of treatment as at the time of the treatment itself,

all those appropriate technical and organizational measures designed to apply,

effectively, the principles of data protection and integrate, in the treatment,

the necessary guarantees to comply with the requirements indicated by the RGPD;

In addition, the person in charge must apply the aforementioned measures to guarantee that, for

default, only the personal data necessary for each specific purpose are processed

of the treatment.

The defendant has stated that the interpretation of the AEPD due to the fact that

Suffering a security breach would automatically imply a breach of the

article 32.1 of the RGPD without providing any motivation regarding the reason why

which security measures are insufficient.

However, it should be noted that such a statement cannot be accepted

since according to the Report prepared by ***EMPRESA.2 it shows 45.-

[……], although it may not be enough for the representative of the respondent

access to some 4,000 credit cards for the purpose of committing fraud; that he

attacker would have collected at least 488847 unique credit cards; that

display and file in ***FILE.1 at least 2651 unique card numbers,

CVVs, expiration dates and cardholder names; than the number

number of records affected were 1,500,000, etc.

Thus, it appears in the antecedents of this proposal and extracted from the

cited report: “In October 2018, GLOBALIA was informed by the companies of

credit cards that a large number of credit cards, some 4,000,

had been used to commit fraud. The stolen data included data

personal and financial of the clients of the claimed person who made reservations and

changes to AirEuropa.com. The data did not include travel data or

passport" that "The first confirmed access to the network of the claimed by the

attacker took place through the CITRIX access gateway by using

valid credentials for an unknown account on May 12, 2018" and

continues by noting that "Following this initial access, the attacker compromised a series of

systems of the claimed considering that the attacker continued accessing the

GLOBALIA systems and accounts at least until August 11, 2018"

Intrusion or unauthorized access 46.-[…….] and that the entity itself could not

detect and that had to be notified by Banco Popular (VISA) when checking

access to customer cards, as evidenced by the claim in

the information sent on 04/01/2019 providing the risk analysis carried out

regarding the need or not to notify this Agency and those interested in the

which is stated: "...once the incident has been identified by the banking entities, these and

the issuers of the compromised bank cards proceeded to block and

inform the interested parties of said block so that the compromised data

were rendered useless…"

Furthermore, the forensic report of ***EMPRESA.3, published

questioned by the defendant's representation also indicates the existence of

evidence of a cardholder data breach, that the exposed data was the

relating to the cardholder's name, address, expiration date and

that their total number was 2722692, etc.

The claim itself in the risk analysis carried out after the incident suffered

points out "In relation to the AIR EUROPA systems, there were no specific measures,

47.-[…….], to protect the data accessed by the attackers…"

The consequence of this lack of adequate security measures was the

unauthorized access to personal data, bank card information,

numbering, expiration date and CVV that could be used to

fraudulent operations as communicated by Banco Popular to the defendant on

***DATE.1.

This mere possibility supposes a risk that has to be analyzed and assessed when

of processing personal data and that increases the demand for the degree of protection in

in relation to the security and safeguarding of the integrity and confidentiality of the

themselves.

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

function of the same to establish the measures that possibly would have prevented the

loss of control of the data and, therefore, by the owners of the data that

they were provided to him as has been credited.

In accordance with what has been indicated, the action of the defendant supposes the violation

of article 32.1 of the RGPD, infringement typified in article 83.4.a).

The defendant has alleged the non-applicability of the RGPD since when

the first access on 05/12/2018, the security requirements were met on that date

required by the applicable legislation at the time of the incident, the LOPD and its

Regulation.

v

However, such an allegation cannot be accepted; the facts subject to the

This claim is subject to the provisions of Regulation (EU)

2016/679, of the European Parliament and of the Council, of 04/27/2016, regarding the

Protection of Natural Persons with regard to Data Processing

Personal and to the Free Circulation of these Data, whose date of full application was

on 05/25/2018.

Access to the personal data of those affected by the bankruptcy began before

from the date of full application of Regulation (EU) 2016/679 -which happens on

05/25/2018- and when the Organic Law 15/1999 on the Protection of

Personal Data, LOPD. However, the defendant's conduct in which

the infraction is specified, breach of security motivated by the adoption of measures

inadequate technical and organizational, has been maintained over time, at least until

the adoption of measures as a result of the communication from Banco Popular to the

claimed and the hiring of forensic companies that caused the implementation

of measures in order to stop the security incident.

It is true that the first access occurs, as the respondent points out, the

05/12/2018 date on which the previous LOPD was in force and that the RGPD is not

full application until 05/25/2018; however, it is not less than the infraction

continued to occur and spread over time until the adoption of those

appropriate measures to put an end to the bankruptcy produced in the systems of the

claimed; It should not be forgotten that the technical and organizational security measures

must be implemented to prevent, among other things, unauthorized access to data

of a personal nature and that these measures must be appropriate.

And although the accesses continued until August 2018, ceasing from

On this date, the measures implemented continued to be inadequate until the

Others were implemented due to the communication of the incident and the adoption of

those new ones due to the intervention of the contracted companies.

The infraction for which the defendant is held responsible participates in the

nature of the so-called permanent infractions, in which the consummation

is projected in time beyond the initial fact and extends, violating the

data protection regulations, during the entire period of time in which the

data is processed. In the present case, despite the fact that on the date on which

the offending conduct began, the applicable norm was the LOPD, the norm that

is applicable is the one that was in force when the infraction ceases to

consummated with the application of those adequate and pertinent measures in order to

that access to personal data could not occur.

The Supreme Court has ruled on the rule to be applied in

those cases in which the infractions are prolonged in time and there have been

a normative change while the infraction was committed. The STS of 04/17/2002 (Rec.

466/2000) applied a provision that was not in force at the initial moment of

commission of the infraction, but yes in the subsequent ones, in which the conduct continued

offending The Judgment examined a case that dealt with the sanction imposed

to a Judge for breach of her duty to abstain in proceedings

Previous. The sanctioned alleged the non-validity of article 417.8 of the LOPJ when

the events occurred. The STS considered that the infraction had been committed

from the date of initiation of the Preliminary Proceedings until the moment in which the

Judge was suspended in the exercise of her functions, so that rule was of

app. The SAN of 09/16/2008 (Rec.488/2006) pronounces in the same sense

SAW

The respondent has alleged that the absence of a response makes him defenseless.

to the evidence presented at the request of the AEPD dated 11/23/2020 and not

have valued them, pointing out, in addition, that it is very harmful that

the AEPD has not taken into consideration a single one of the allegations made

nor has it taken into account even one of the documents provided in the answer

to the requirement issued by the AEPD during that evidentiary phase.

The alleged defenselessness cause is surprising; It should be noted that if it was not done

reference to them was due to the fact that the answer offered did nothing but

consolidate and reinforce the reports provided by IBM and Foregenix that companies

measures implemented at the time and moment of the bankruptcy produced were not the most

suitable for data security.

Measures that must be established by the data controller

taking into account the risk analysis carried out and based on it, apply

the most appropriate technical and organizational measures.

Thus, in the first place a series of network diagrams of the environment of

payments, but the place where each type of data was stored, where

each specific type of data was stored.

In his statements, the respondent pointed out that the data of a

personnel of those affected (postal addresses, telephone, passport, DNI, date

birth, etc.), were stored independently of the information related to

to bank cards and that, therefore, the aforementioned data was not compromised.

However, it is also not proven that the data relating to the owner of the data and

therefore those related to the cards were filed separately; the report itself

audit report of ***COMPANY.2 indicates that “The attacker viewed and filed in

***FILE.1

(…) at least 2651 unique card numbers, CVVs, dates of

expiration date and names of the card holder”. And in the same report it is also

states that “The stolen data included personal and financial data of the

GLOBALIA customers who made reservations and changes in ***URL.1. The

data did not include travel or passport data” (the underlining corresponds to the

AEPD).

And the respondent herself in her response dated 12/16/2020 stated that

“As can be seen, neither the databases of the environment object of this

research, nor the potential data compromise, included information that was not

the one already indicated; that is, unique card numbers, CVVs, expiration dates and

cardholder names. That is, it was implicitly recognizing that

the name of the holder was included in the data within the potential compromise of

data, which should have been relevant when establishing the need to give

to diligently notify the security incident to the AEPD, given

the importance of the data that could or could not be accessed.

Regarding the risk analyses, the last document presented by the

claimed is dated 06/04/2020 on the occasion of the EIPD, more complete than the

presented on 04/01/2019. The one contributed in the first place does not determine what level of

risk is or is not acceptable for the treatment carried out, nor do they determine its

calculation, nor does it break down the mitigating measures, etc., compared to the last

presented (where, if measures such as double authentication and

strong passwords that are implemented in the Risk Analysis).

The respondent alleges that when the security incident began, no

applied the RGPD and that the measures proposed in the Risk Analysis in that

time were in accordance with existing recommendations at the time.

However, it should be noted that in relation to two types of measures,

48.-[……] to which the respondent alludes recommends "49.-[……]", that is, what

which was already established in the reports of the companies involved and which appears

reflected in the report of previous actions and, in terms of the length and complexity

of the password, in the same previous report (that of CNN) it is pointed out and recommended

fifty.-[……].

As for 51.-[……], he states that he was completely updated to

date of the incident and present a supporting document. However, 52.-[……].

As far as 53.-[……] as a measure implemented at the time of the incident

According to the respondent, it is due to the fact that in the CCN report referred to

above states that the length of passwords must be at least 8

with different types of characters and that these recommendations were already met

01/17/2018 following their recommendations and providing a screenshot with the

password policy where it states that "passwords must meet the requirements

of complexity", "enabled", "minimum password length" and "8 characters".

However, it is not appreciated, accredited or justified what kind of complexity

enabled is referring and in any case, in the report of *** COMPANY.2 it is

points out that "subsequent investigations of the accounts compromised by the

attacker, such as the service account ***SERVICE.1, revealed that he was using a

password that did not meet the complexity and length requirements in line with the

industry best practice, which would have made it easier for the attacker to

easy to compromise this account."

In relation to 54.-[…….] they point out that they were XXXXXXXX presenting

the network diagram.

However, the report of ***EMPRESA.3 of January 2019 referred to

because the server 55.-[…….], "The attack began when the attacker accessed 56.-

[…….]" and "Although there were XXXXX and XXXXX, the attacker was able to "pivot" the entry 57.-

[…….]"

Finally, in relation to the blocking of external IPs that are not related

with no payment system pointed out that "It was not technically possible to limit the

IP's of the various authorization centers. Therefore, outgoing connections (not so

starters) were not, nor could they be, restricted."

However, neither is credited nor is any information given as to why

was technically possible or why it was not possible to limit the IPs.

7th

The respondent alleges in relation to the report provided by ***COMPANY.3 that

it is not an expert report, nor an objective technical report, 58.-[…….], with the

in order to calculate the amount of compensation that this regulatory environment requires from

associated entities in certain situations and that there is an incompatibility

between the purposes of that report and those to be pursued in a

sanctioning administrative file.

However, such an allegation cannot be accepted either: firstly, because

the respondent has not provided any evidence of his bias, which might have

provoked his challenge, without proof having been accredited in the procedure

any of it.

And secondly, because the Report issued by the aforementioned company states:

1. This investigation is carried out in strict compliance with all the

applicable requirements set forth in Section 2.3 of the Requirements relating to the

PCI forensic investigator qualifications, including, without limitation,

requirements set forth in said section relating to independence, professional opinion,

integrity, objectivity, impartiality and professional skepticism.

2. This Preliminary Incident Response IPP Report identifies,

describes, represents and characterizes all the objective evidence that the PFI Company

and its Employees collected, generated, discovered, analyzed and/or considered

its sole discretion relevant to this investigation in the course of conducting the

same.

3. The opinions, conclusions and findings contained in this Report

Preliminary Incident Response IPP (a) accurately reflect and are based on

exclusively on the objective tests described above, (b) reflect only

the opinions, conclusions and findings of the PFI Company and its Employees,

acting in its sole discretion, and (c) have not been influenced, directed, controlled,

modified, proportionate or subject to the prior approval of the object Entity

of Research or any contractor, representative, professional adviser, agent or

affiliate of the same or any other person or entity other than the PFI Company and

its Employees (the underlined corresponds to the AEPD).

Secondly, the defendant is charged with the violation of article 33 of the

RGPD, Notification of a violation of the security of personal data to the

control authority, which establishes:

viii

"1. In case of violation of the security of personal data, the

responsible for the treatment will notify the competent control authority of

accordance with article 55 without undue delay and, if possible, no later than 72

hours after you become aware of it, unless it is unlikely

that said breach of security constitutes a risk to the rights and

freedoms of natural persons. If the notification to the control authority does not have

place within 72 hours, must be accompanied by an indication of the reasons for

the procrastination

2. The person in charge of the treatment will notify the person in charge without undue delay

of the treatment the violations of the security of the personal data of which

be aware.

3. The notification referred to in section 1 must, at a minimum:

a) describe the nature of the data security breach

including, where possible, the categories and number

approximate number of stakeholders affected, and the categories and approximate number

of affected personal data records;

b) communicate the name and contact details of the data protection delegate

data or another point of contact where further information can be obtained;

c) describe the possible consequences of the breach of the security of the

personal information;

d) describe the measures adopted or proposed by the person responsible for the

processing to remedy the data security breach

including, if applicable, the measures taken to mitigate the

possible negative effects.

4. If it is not possible to provide the information simultaneously, and to the extent

where it is not, the information will be provided gradually without undue delay.

5. The data controller will document any violation of the

security of personal data, including the facts related to it, its

effects and corrective measures taken. Such documentation will allow the

control authority verify compliance with the provisions of this article.

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

April 2016, regarding the protection of natural persons with regard to

treatment of personal data and the free circulation of these data and by which

repeals Directive 95/46/EC (General Data Protection Regulation), (as regards

successive RGPD) defines security breaches of personal data as

those incidents that cause the accidental destruction, loss or alteration or

illicit personal data, as well as unauthorized communication or access to the

themselves.

Since last 05/25/2018, the obligation to notify the Agency of breaches

or security breaches that could affect personal data is applicable to

any controller of personal data processing, which underlines the

importance that all entities know how to manage them.

In this sense, recital 87 establishes that:

“It must be verified if all the adequate technological protection has been applied and appropriate organizational steps have been taken to determine immediately whether there has been a violation of the security of personal data and to report without delay to the supervisory authority and the interested party. It must be verified that the notification has been made without undue delay taking into account, in particular, the nature and seriousness of the violation of the security of the personal data and its consequences and adverse effects for the interested party. Such notice may result in an intervention of the supervisory authority in accordance with the functions and powers established by this Regulation.

Regardless of the actions of an internal nature that were carried out carried out by the claimed party to manage the breach or security incident once knowledge of it, the RGPD establishes that in the event of a breach of the security of personal data, the data controller will notify the competent supervisory authority without undue delay and, if possible, no later than 72 hours after you become aware of it, unless it is unlikely that said security breach constitutes a risk to the rights and freedoms of natural persons.

The RGPD also establishes the cases in which a security breach is must notify the affected party, specifically when it is likely that the breach of the security of personal data entails a high risk for the rights and freedoms of natural persons.

Both the notification to the competent control authority and the communication to the affected party are obligations of the data controller, although You can delegate their execution to other figures.

Therefore, what underlies this obligation is a broader duty and that urges the person in charge to implement a procedure for managing incidents of

security that affect personal data adapted to the characteristics of the

treatment.

Therefore, a key element of any policy on

data security is being able, to the extent possible, to prevent a breach and,

when, despite everything, it occurs, react quickly.

The RGPD points out that breaches are those incidents that cause the

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

unauthorized communication or access to them.

In the case examined, the documentation provided in the file

offer clear indications of the existence of a security incident provoked and

suffered in the entity's systems, classified as a breach involving access

unauthorized access to user data, specifically information relating to data

personal, bank cards, numbering, expiration date and CVV that could be

have used for the commission of fraudulent operations and that in accordance

with what is indicated in the previous foundation would violate article 32.1 of the RGPD,

Security of the treatment, of which the person claimed by the

communication received from financial entities causing the activation of the

response to incidents (IRP) the next day.

The respondent adopted the decision to notify this control authority of the

security breach detected on 11/27/2018, through the form enabled in

electronic headquarters but the online procedure made it impossible to present it, so

it had to be done the next day, on 11/28/2018 in person.

It is true, as the defendant's representation shows that there was

notification of bankruptcy, although this was carried out 41 days out of time

after it was known in clear violation of the provisions of article 33

of the RGPD that establishes the obligation to notify the control authority without delay

undue and, at the latest, 72 hours after you have become aware of it.

The respondent justifies the late notification made because there was no

Sufficient knowledge of the nature or scope suffered and that it would have affected

personal information.

However, such an allegation cannot be admitted since the person responsible for the

treatment had clear evidence that such a violation had occurred and there was no

doubts that he was aware of it as a result of the Bank's notification

Popular on ***DATE.1 that caused the activation as previously indicated

of the incident response plan the next day. This is how it appears in the IBM report

“In October 2018, GLOBALIA was informed by credit card companies

credit that a large number of credit cards, some 4,000, had been

used to commit fraud.

In addition, if it were true what the respondent himself states in his writ of

date 01/22/2019 where it states that the bankruptcy was solved on 11/17/2018,

Why didn't you notify him earlier?

Moreover, in the risk analysis carried out regarding the need or not of

notification to the Agency, in conclusions, it is stated that "Applying the methodology of

analysis of the AEPD to the current incident (Annex 1), both the quantitative result and

the qualitative exceed the threshold of notification to the AEPD…”

On the other hand, the investigations and analyzes carried out by the entity did not

classified the incident as a high risk for the rights and freedoms of the

stakeholders, so the bankruptcy, which affected 1,500,000 data records

approximately and approximately 489,000 users, those affected were not notified

since there was only a record of 20 requests for information by

customers responding to all of them. In the conclusions of risk analysis

above, it is stated that “In relation to the notification to interested parties and according to the

analysis methodology of the AEPD (Annex 1), the quantitative result would not exceed the

threshold established for said notification (30 vs. 40), while the threshold

qualitative yes it would be overcome”.

In accordance with the preceding paragraphs, the actions of the respondent

supposes the violation of 33.1 of the RGPD, an infraction typified in its article 83.4.a)

of the same legal text.

IX

The violation of articles 32.1 and 33 of the RGPD are typified in

Article 83.4.a) of the aforementioned RGPD in the following terms:

"4. Violations of the following provisions will be sanctioned, in accordance

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

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

global total annual turnover of the previous financial year, opting for

the largest amount:

a)

the obligations of the person in charge and the person in charge in accordance with articles 8,

11, 25 to 39, 42 and 43.

(…)

For its part, the LOPDGDD in its article 71, Violations, states 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.

And in its article 73, for the purposes of prescription, it qualifies as "Infringements

considered serious”:

“Based on the provisions of 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:

(…)

g) The violation, as a consequence of the lack of due diligence,

of the technical and organizational measures that have been implemented in accordance with

required by article 32.1 of Regulation (EU) 2016/679”.

r) Failure to comply with the duty to notify the data protection authority

data of a breach of security of personal data in accordance with the

provided for in article 33 of Regulation (EU) 2016/679.

The accredited facts show the existence of a security breach

in the systems of the claimed allowing its vulnerability causing access not

authorized and unlawful access to information relating to customers in relation to their cards

bank numbers, numbering, expiration date and CVV that could have been used to

the commission of fraudulent operations, which together with the extemporaneous notification

of the aforementioned breach or security incident supposes the infraction of articles 32.1

and 33 of the RGPD.

X

In order to establish the administrative fine to be imposed,

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

point out:

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

administrative actions under this article for violations of this

Regulation 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 as a substitute for the measures contemplated

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

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

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

nature, scope or purpose of the processing operation in question

as well as the number of stakeholders affected and the level of damage and

damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;

d) the degree of responsibility of the person in charge or of the person in charge of the

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

applied under articles 25 and 32;

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

treatment;

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

remedying the breach and mitigating the possible adverse effects of the breach;

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

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

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

what extent;

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

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

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

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

certificates approved in accordance with article 42, and

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

case, such as financial benefits realized or losses avoided, direct

or indirectly, through infringement.

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

Article 76, “Sanctions and corrective measures”, establishes that:

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

2016/679 may also be taken into account:

a) The continuing nature of the offence.

b) The link between the activity of the offender and the performance of treatments

of personal data.

c) The profits obtained as a result of committing the offence.

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

commission of the offence.

data.

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

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

f) Affectation of the rights of minors.

g) Have, when it is not mandatory, a delegate for the protection of

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

voluntary, to alternative conflict resolution mechanisms, in those

assumptions in which there are controversies between those and any

interested."

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

sanction to be imposed in the present case for the infractions typified in article

83.4.a) of the RGPD for which AIR EUROPA is responsible, it is estimated

concurrent the following factors:

- In relation to the infringement of article 32.1 of the RGPD typified in the

Article 83.4 of the aforementioned Regulation:

The nature and seriousness of the infringement given its not merely local scope

of the declared security breach, but quite the opposite since they have been able to

see compromised personal data not only of nationals but foreigners,

without forgetting the high number of people, customers, potentially affected by the

same (489,000) and the number of records affected (1,500,000); in the IBM report

of 12/20/2018 it was noted that "GLOBALIA was informed by the companies of the

credit cards that a large number of credit cards, some 4,000, had

been used to commit fraud", "Although IRIS has not been able to confirm how it managed to

the attacker to exfiltrate information from the GLOBALIA network or what was exfiltrated, given

account of the limitation of records, what IRIS has confirmed is that the attacker

had collected at least 488,847 unique credit cards" and in the report of

***COMPANY.3 provided by the respondent on 11/14/2019, it was stated that "The

***COMPANY.3 research identified more than 2.7 million card numbers

unique that had been extracted from the database systems by the attacker";

the category of data affected by the infringement, without forgetting the damages

suffered by some of the clients.

The degree of responsibility of the data controller, taking into account

the technical or organizational measures applied and that were violated. A) Yes,

***EMPRESA.2 indicates that "…, the attacker took advantage of 59.-[……] to get

access the network for the first time", that "Any system exposed to the Internet, 60.-[……]

"…, subsequent investigations of the accounts compromised by the attacker,

***SERVICE.1, revealed that it used a password that did not meet the requirements of

complexity and length in line with industry best practice, which would have

made it easier for the attacker to compromise this account."

***EMPRESA.3 in its report states that "The intrusion probably had

its origin in insecure systems available through the internet. ***COMPANY.3

identified several devices that had not been regularly patched…",

But the claimed entity itself has indicated that "In relation to the systems

of AIR EUROPA, there were no specific measures, such as encryption or tokenization,

to protect the data accessed by attackers. However, the

information accessed by the attackers does not include sensitive information such as

special categories of personal data, postal addresses or telephone numbers

telephone, passport number or DNI or date of birth. This sensitive information

is not stored together with bank card information as a security measure.

security. As a result, it is very difficult to identify unique individuals within the

data set."

The categories of personal data that have been affected

as a consequence of the infraction because to the identification data it is necessary to add the

banking and financial, as a result of access to the cards, with a purpose

clearly fraudulent. In the audit report made by ***EMPRESA.2 of

12/20/2018 states that “In October 2018, GLOBALIA was informed by the

credit card companies that a large number of credit cards,

some 4,000 had been used to commit fraud. The stolen data included

personal and financial data of GLOBALIA customers who made reservations and

modifications in ***URL.1” (the underlined corresponds to the AEPD).

The way in which the infraction was known, since it was due to

a communication from BANCO POPULAR, and as indicated in the previous paragraph by

credit card companies, without the claimant having had proof of the

intrusion and committed accesses that began on 05/12/2018.

The continuing nature of the infringement in the sense interpreted by the

National High Court as a permanent infraction, since since the

security incident until the breach was detected, a period of

time of several months.

The activity of the allegedly infringing entity is linked to the

data processing of both customers and third parties; the quoted is known

link since the entity, due to its activity, is in permanent contact with

customers and third parties dealing with a large volume of data, which imposes a greater

duty of diligence.

The volume of business of the claimed company since it is one of the company

leader in the Spanish market, in its business object air transport; the

claimed forms part of the business holding company Globalia Corporación Empresarial S.A.

and of which a large number of companies are part, having had income

annual of

€2,367,061,000 (2018) and €2,130,517,000 (2019) and a result of

exploitation of €82,921,000 (2018 and €93,984,000 (2019) as stated on page

website of the corporate group and according to the last publication of the BORME on 12/30/2020 a

share capital of €17,923,050.

For all these reasons, an amount of the penalty is established for violation of the

article 32.1 of the RGPD of 500,000 euros.

In relation to the circumstances of the responsibility, the respondent has

alleged that the application

of mitigating circumstances, considering that if the infraction is understood to have been committed

of article 32.1, the following extenuating circumstances would apply: the

low seriousness of the incident and the low level of damage caused; measures

taken by the person responsible to alleviate the damages suffered; The cooperation

with the control authority and the lack of benefits obtained.

However, such a claim cannot be accepted; the circumstances

aggravating circumstances that have been taken into account are those that occur in this case.

Regarding the seriousness of the infraction, it already concurs as an aggravating circumstance in the Gradation of the sanction for infraction of article 32.1: “The nature and seriousness of the infringement given its not merely local scope of the security breach declared, but quite the opposite since data may have been compromised of a personal nature not only of nationals but foreigners, without forgetting the high number of people, customers, potentially affected by it (489,000) and the number of records affected (1,500,000); in the report of ***COMPANY.2 of 12/20/2018 it was noted that…”

In addition, it is striking that the infraction is classified as of little seriousness committed when the LOPDGDD itself in its article 73 considers it for the purposes of prescription as a serious infraction and when the lack of compliance is evident and palpable. diligence in applying the appropriate measures of a technical and organizational, extending from 05/12/2018 date of first access until Appropriate measures were implemented at the request of the contracted companies.

As for the low level of damage caused as a result of the infraction, it is not predicable to the present case where there are also injured parties, but even if there were not, we are faced with the infringement of a fundamental right and the high degree of interference in customer privacy must be taken into account this being enough damage for them.

Even more striking is the request that the adoption of measures taken by the person responsible to mitigate the damages and

cooperation with the supervisory authority, when they are nothing more than legal obligations

that must be required of any person responsible for and in charge of the treatment and, more

when, as indicated above, the lack of diligence in the

application of the same to prevent unauthorized access, although it is true that their

non-compliance could lead to its application as aggravating circumstances.

And as for the absence of benefits, it is inadmissible; the GDPR is

refers to the profits obtained as a result of committing the offence,

not that the absence of benefits should be considered as extenuating.

Therefore, assessing the concurrent circumstances and taking into account

consideration especially those that operate as aggravating factors and that have been analyzed

above, the sanction imposed by

violation of article 32.1 of the RGPD, given the seriousness of the events that occurred

- In relation to the infringement of article 33 of the RGPD typified in article

83.4 of the aforementioned Regulation:

The serious lack of diligence in complying with the obligations imposed

by the data protection regulations, making an extemporaneous notification of

the bankruptcy of security to which he was obliged.

The way in which the infraction was known, since it was due to

a notification from BANCO POPULAR and by credit card companies, without

the defendant would have been aware of the intrusion and accesses committed that

They started on 05/12/2018.

The activity of the allegedly infringing entity is linked to the

data processing of both customers and third parties; the quoted is known

link since the entity for its activity is in permanent contact and treats a

large volume of data, which imposes a greater duty of care.

The volume of business of the claimed company since it is one of the company

leader in the Spanish market, in its business object.

For all these reasons, an amount of the penalty is established for violation of the

article 33 of the RGPD of 100,000 euros.

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of sanctions whose existence has been proven,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE AIR EUROPA LINEAS AÉREAS S.A., with CIF ***CIF.1, for

an infringement of article 32.1 of the RGPD, typified in Article 83.4.a) of the RGPD,

a fine of €500,000 (five hundred thousand euros).

SECOND: IMPOSE AIR EUROPA LINEAS AÉREAS S.A., with CIF ***CIF.1, for

an infringement of article 33 of the RGPD, typified in article 83.4.a) of the RGPD, a

fine of €100,000 (one hundred thousand euros).

THIRD: NOTIFY this resolution to AIR EUROPA LINEAS AÉREAS S.A.

FOURTH

: Warn the sanctioned person that he must make the imposed sanction effective once

Once this resolution is enforceable, in accordance with the provisions of the

art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (hereinafter LPACAP), within the payment term

voluntary established in art. 68 of the General Collection Regulations, approved

by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,

of December 17, through its entry, indicating the NIF of the sanctioned and the number

of procedure that appears in the heading of this document, in the account

restricted number ES00 0000 0000 0000 0000 0000, opened on behalf of the Agency

Spanish Department of Data Protection in the banking entity CAIXABANK, S.A.. In case

Otherwise, it will be collected in the executive period.

Received the notification and once executed, if the date of execution is

between the 1st and 15th of each month, both inclusive, the term to make the payment

voluntary will be until the 20th day of the following month or immediately after, and if

between the 16th and last day of each month, both inclusive, the payment term

It will be until the 5th of the second following month or immediately after.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once it has been notified to the interested parties.

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.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es