 Procedure No.: PS/00144/2020

RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection and with

based on the following

BACKGROUND

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

notification of security breach of personal data sent by VOX ESPAÑA

(hereinafter VOX) in which the Spanish Data Protection Agency is notified

(hereinafter AEPD) that, on September 20, 2019, have had

knowledge through the Cybersecurity Institute (hereinafter INCIBE) of the

publication in a digital medium of links where a theft of information is revealed

VOX affiliate data information.

By bringing VOX to the attention of the Civil Guard Telematic Crimes Group

these facts, informs them that, after having carried out investigations, the information

published figure corresponds to a previous incident already notified to the AEPD in

dated 12/13/2018, regarding the publication of a link in which subscribers appear

of VOX news on its website.

In the present case, according to VOX, the second security breach now

notified refers to the attack on a VOX computer team assigned to a leader

of VOX in Barcelona (Sabadell) from which a file with data from

affiliates

the web address

https://keybase.pub/anoncatalonia/VOX/.

party and published

in

to the

In this second notification (dated 09/25/2019), VOX has provided a letter sent

to the affected affiliates where they are informed that one of the leaders of Catalonia

(Sabadell) has suffered an attack on the computer equipment assigned to it, which has

allowed access to a temporary file with data of affiliates of the town of

Sabadell.

SECOND: In view of the aforementioned data security breach notification

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

of previous investigation actions, having knowledge of the following

ends:

BACKGROUND

Date of notification of security breach of personal data: 25 of

september 2019

INVESTIGATED ENTITIES

VOX ESPAÑA, with NIF G86867108 and with address at C/ Bambú 12, 28036 Madrid.

RESULT OF THE INVESTIGATION ACTIONS

Regarding the first security breach of personal data (dated

12/13/2018) informed to VOX by INCIBE and related to an attack on the VOX website,

preliminary proceedings were opened with reference E/10207/2018 motivated by

the notification sent to the AEPD by VOX in which a

cyberattack by the group La Nueve de Anonymous against the VOX website, having as

result in posting a link to news subscribers.

Regarding the second security breach of personal data (notified to the

AEPD on 09/25/2019) now analyzed against a VOX computer assigned to

a leader regarding access to affiliate data in Sabadell:

1. On October 4, 2019, from the Data Inspection you access the

web address https://keybase.pub/anoncatalonia/VOX/ obtaining as a result

"Page not found".

VOX has provided screen printing of the information available on

https://keybase.pub/anoncatalonia/VOX/ at the time of communication of the

INCIBE and the reference to the file “afiliados_sabadelll.xlsx” appears.

2. With dates October 9, 2019 and March 6, 2020, information is required to

VOX and, from the response received on October 24, 2019 and March 17,

2020, the following follows:

Regarding the chronology of events. Incidence minimization measures

□

On September 21, 2019, INCIBE informed VOX of the access

by cybercriminals to data of VOX affiliates that were published in the

profile of Anonymus Catalonia (@anonktalonia). In that link there were

subscriber data from a previous attack in 2018 (actions by

reference E/10207/2018) and a document in Excel format with data from

affiliated to the party in Sabadell.

We proceeded to study said Excel file, verifying that the data were

extracted from the personal computer of a VOX leader in Barcelona (Sabadell).

□

□

On September 22, the leader of VOX in Barcelona filed a complaint

before the Civil Guard, which proceeded to block all links to the website of

VOX. In this regard, VOX has filed a complaint with the Crimes Group

Telematics of the Civil Guard dated September 22, 2019.

On this same date, the security breach was reported.

to those affected.

Regarding the causes that made possible the incidence

 VOX states that the security measures of the

computer assigned to the leader of Barcelona, which has allowed

outside third parties could access a temporary file that contained the

Sabadell affiliate data.

 VOX states that in the documents signed by the leaders of the party

Regarding confidentiality and the duty of secrecy, the

maintenance of temporary files with affiliate data.

In this regard, Vox has provided “Confidentiality and professional secrecy agreement.

Person authorized for data processing” dated February 2, 2018

signed by the leader whose computer was hacked.

Regarding the security measures implemented prior to the incident

 VOX has provided a status report and system security audit

to verify compliance with the legislation on the protection of

data according to the notification of the aforementioned file and the result of the

audit is “Compliance”. This report is confidential and

is included in the file.

THIRD: On June 16, 2020, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimant, for the

alleged infringement of Article 32 of the RGPD, typified in Article 83.4 of the RGPD.

FOURTH: On October 2, 2020, a resolution proposal was formulated, in which

what was proposed,

<<That by the Director of the Spanish Data Protection Agency:

 VOX ESPAÑA, with NIF G86867108, is sanctioned for infraction of Article

32.1, b) in relation to article 5.1.f) of the RGPD, in accordance with the provisions

in article 83.4 of the RGPD, considered a serious infringement for the purposes of

prescription in article 73.g) of the LOPDGDD, and for infraction of article

5.1.f) of the RGPD, in accordance with the provisions of article 83.5 of the

RGPD, considered a very serious infringement for the purposes of prescription in the

Article 72.1.i) of the LOPDGDD, with a warning.

 VOX ESPAÑA, with NIF G86867108, is required to implement in the system

of information for which it is responsible, the appropriate measures to avoid

the future the repetition of events similar to the one analyzed in the present

procedure.>>

FIFTH: The investigated entity has not submitted allegations to the Proposal for

Resolution.

In view of everything that has been done, by the Spanish Data Protection Agency

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST: VOX acknowledges and is thus accredited that, on 09/20/2019, it has

suffered an external attack against the VOX computer team assigned to a leader

in Barcelona (Sabadell) from which a file with data on members of the

match and subsequently posted to the attacker's web address

https://keybase.pub/anoncatalonia/VOX/.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

4/10

SECOND: It is recorded that VOX has communicated to the affected affiliates that one of the

computer equipment for which it is responsible has suffered an external attack that has

allowed the access and publication of the data of the members of the party on the Internet by

outside third parties.

FOUNDATIONS OF LAW

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

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

The Spanish Agency for Data Protection is competent to resolve this

process.

Yo

Article 5 of the RGPD establishes the following:

II

"1. The personal data will be:

a) processed in a lawful, loyal and transparent manner in relation to the interested party ("lawfulness,

loyalty and transparency»);

b) collected for specific, explicit and legitimate purposes, and will not be processed

subsequently in a manner incompatible with those purposes; according to article 89,

paragraph 1, the further processing of personal data for archiving purposes in

public interest, scientific and historical research purposes or statistical purposes are not

deemed incompatible with the original purposes ("purpose limitation");

c) adequate, pertinent and limited to what is necessary in relation to the purposes for which

that are processed ("data minimization");

d) accurate and, if necessary, updated; all measures will be taken

reasonable to eliminate or rectify without delay the personal data that

are inaccurate with respect to the purposes for which they are processed (“accuracy”);

e) kept in a way that allows the identification of the interested parties during

longer than necessary for the purposes of the processing of personal data; the

Personal data may be kept for longer periods provided that it is

processed exclusively for archival purposes in the public interest, research purposes

scientific or historical or statistical purposes, in accordance with Article 89, paragraph 1,

without prejudice to the application of the appropriate technical and organizational measures that

This Regulation is imposed in order to protect the rights and freedoms of the

interested party (“limitation of the retention period”);

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

including protection against unauthorized or unlawful processing and against

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

or appropriate organizational ("integrity and confidentiality").

2. The controller will be responsible for compliance with the provisions

in section 1 and able to demonstrate it (“proactive responsibility”).”

Article 4.12 of the RGPD establishes that it is considered “violation of the security of the

personal data": any breach of security that results in the destruction, loss

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

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

III

Article 33.1 of the RGPD establishes the following:

"In case of violation of the security of personal data, the person in charge of the

treatment will notify the competent control authority in accordance with the

article 55 without undue delay and, if possible, no later than 72 hours after

who was aware of it, unless it is unlikely that such violation

constitutes a risk to the rights and freedoms of individuals

physical. If the notification to the supervisory authority does not take place within the period of 72

hours, must be accompanied by an indication of the reasons for the delay."

IV

From the actions carried out, it can be deduced that VOX informed this AEPD within

within 72 hours of being aware of the personal data security breach

-according to article 30 of Law 39/2015, of October 1, of the Procedure

Common Administrative of Public Administrations- giving, consequently,

compliance with the provisions of article 33.1 of the RGPD

Article 32 of the RGPD establishes the following:

.

"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 the availability and access to the personal data of

quickly in the event of a physical or technical incident;

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

technical and organizational measures to guarantee the security of the treatment.

1. When evaluating the adequacy of the security level, particular account shall be taken of

takes 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." (The underlining is from the Spanish Agency

Data Protection).

Article 28 of the LOPDGDD establishes the following:

v

"1. Those responsible and in charge, taking into account the elements

listed in articles 24 and 25 of Regulation (EU) 2016/679, will determine the

appropriate technical and organizational measures that must be applied in order to guarantee and

prove that the treatment is in accordance with the aforementioned regulation, with this law

organization, its implementing regulations and the applicable sectoral legislation. In particular

They will assess whether it is appropriate to carry out the impact assessment on the protection of

data and the prior consultation referred to in Section 3 of Chapter IV of the aforementioned regulation.

2. For the adoption of the measures referred to in the previous section, the controllers and processors shall take into account, in particular, the greater risks that could occur in the following cases:

a) When the treatment could generate situations of discrimination, identity theft or fraud, financial loss, reputational damage, loss of confidentiality of data subject to professional secrecy, reversal not authorized pseudonymization or any other economic, moral or social damage significant for those affected.

b) When the treatment could deprive those affected of their rights and freedoms or could prevent them from exercising control over their personal data.

c) When the treatment is not merely incidental or accessory of the special categories of data referred to in articles 9 and 10 of the Regulation (EU) 2016/679 and 9 and 10 of this organic law or related data with the commission of administrative infractions." (…)

Recitals 51 and 75 of the RGPD establish the following:

SAW

(51) Special protection deserves personal data that, by their nature, is particularly sensitive in relation to fundamental rights and freedoms, as the context of their treatment could entail significant risks for the fundamental rights and freedoms.

(75) The risks to the rights and freedoms of natural persons, serious and variable probability, may be due to the processing of data that could cause physical, material or immaterial damages, in particular (...) in cases where which the treatment may give rise to problems of discrimination, usurpation of

identity or fraud; in cases in which the interested parties are deprived of their rights

and freedoms or are prevented from exercising control over your personal data; In the cases

in which the personal data processed reveal ethnic or racial origin, opinions

policies, (...)

Of the actions carried out, it has been verified that the security measures with which

that the investigated entity had in relation to the data that it submitted to

treatment as responsible, were not adequate at the time of

breach of personal data security occurs, with the consequence of the

public exposure on the internet of the personal data of affiliates of the town of

Sabadell. In other words, those affected affiliated with VOX in that locality have been

deprived of control over their personal data by making public a

particular position or political ideology whose public disclosure is not intended to

what to have been consented by its holder.

This possibility represents a risk that must be weighed when treating

certain data with a special category as indicated in article 9 of the RGPD, and

which increases the demand for the degree of protection in relation to safety and

safeguarding the confidentiality of these data.

This risk must be taken into account by the controller and depending on

establish the measures that would have prevented the loss of control of the

data by the data controller and, therefore, by the owners

of the data that they provided to it.

From the actions carried out, it can be deduced that VOX, at the date of notification of the security breach, it did not have adequate security measures in its information systems in accordance with the provisions of article 32 of the RGPD, in relation to article 28 of the LOPDGDD.

Article 71 of the LOPDGDD establishes, under the heading "Infractions" the following:

The acts and behaviors referred to in sections 4, 5 constitute infractions. and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result contrary to this organic law.

7th

It establishes article 72 of the LOPDGDD, under the rubric "infractions considered very serious" the following: "1. Based on the provisions of article 83.5 of the Regulation (EU) 2016/679 are considered very serious and will expire after three years infractions that suppose a substantial violation of the articles mentioned therein and, in particular, the following:

a) The processing of personal data violating the principles and guarantees established in article 5 of Regulation (EU) 2016/679".

In the present case, the circumstance provided for in article 72.1.a) of the LOPDGDD indicated above.

It establishes article 73 of the LOPDGDD, under the heading "Infringements considered serious" the following: "According to what is established in article 83.4 of the Regulation (EU) 2016/679 are considered serious and will prescribe after two years the infractions that suppose a substantial violation of the articles mentioned in that and, in particularly the following:

(…)

f) The lack of adoption of those technical and organizational measures that are appropriate to guarantee a level of security appropriate to the risk of the treatment, in the terms required by article 32.1 of the Regulation (EU) 2016/679."

In the present case, the circumstance established in article 73.f) of the LOPDGDD indicated above.

This lack of diligence in implementing adequate security measures in the VOX computers that it assigned to its leaders constitute the element of guilt that requires the imposition of a sanction.

viii

Likewise, the lack of consideration of the risk that access may entail does not authorized by third parties to affiliate data related to a political party and its subsequent public dissemination aggravates the guilt and sanctioning reproach of the behavior carried out by VOX.

Article 58.2 of the RGPD establishes the following:

IX

2. Each supervisory authority will have all of the following powers corrections listed below:

(…)

b) sanction any person responsible or in charge of the treatment with warning when the processing operations have violated the provisions of this Regulation;

(…)

Establishes article 76 of the LOPDGDD under the heading "Sanctions and measures corrective measures", states the following:

1. The penalties provided for in sections 4, 5 and 6 of article 83 of the Regulation (EU) 2016/679 will be applied taking into account the criteria of graduation established in section 2 of the aforementioned article.

2. 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 personal data processing.

c) The benefits obtained as a result of the commission of the infringement.

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

e) The existence of a merger process by absorption subsequent to 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 data.

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 them and any interested party.

2. It will be possible, complementary or alternatively, the adoption, when appropriate, of the remaining corrective measures referred to in article 83.2 of the Regulation (EU) 2016/679".

From the foregoing, it is clear that VOX has violated article 32.1, b) in relation to the article 5.1.f) of the RGPD, infringement typified in article 83.4 of the RGPD, considered a serious infringement for prescription purposes in article 73.g) of the LOPDGDD, and article 5.1.f) of the RGPD, infringement typified in article 83.5 of the RGPD, considered a very serious infringement for the purposes of prescription in the article 72.1.a) of the LOPDGDD.

In the present case, in view of the diligence carried out by VOX in relation to to the notification without undue delay of the security breach to this AEPD, as well as communication to the interested parties and the initiation of actions aimed at minimizing the negative consequences of the aforementioned breach of security, is considered in accordance with right not to impose a sanction consisting of an administrative fine and replace it with the penalty of warning in accordance with the provisions of article 76.3 of the LOPDGDD in relation to article 58.2 b) of the RGPD.

Therefore, in accordance with the applicable legislation and having assessed the criteria for graduation of the sanctions whose existence has been proven, the Director of the Spanish Data Protection Agency RESOLVES:

FIRST:

1.

IMPOSE VOX ESPAÑA, for violation of Article 32.1, b) in relation to article 5.1.f) of the RGPD, in accordance with the provisions of article 83.4 of the RGPD, and for violation of article 5.1.f) of the RGPD, in accordance with the provided in article 83.5 of the RGPD, a sanction of warning.

2. REQUEST VOX ESPAÑA, to implement in the information system of the

that it is responsible for the appropriate measures to avoid future repetition

of facts similar to the one analyzed in this procedure and notify

this Agency such measures within a period of three months.

SECOND: NOTIFY this resolution to VOX ESPAÑA, with NIF G86867108

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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