* Procedure No.: PS/00254/2019

938-300320

RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following

BACKGROUND

FIRST: On 12/13/2018 a bankruptcy notice is received

security sent by VOX ESPAÑA (hereinafter VOX) in which they inform that

have learned, through social networks, of a computer attack

carried out by the Group ***GRUPO.1, on December 12, 2018 at 7:30 p.m., which

has allowed access to the entity's news subscriber database.

The information accessed corresponds to basic data and VOX considers that it can

about thirty thousand affected

Upon learning of the facts, VOX contracted a specialized forensic service and

proceeded to isolate the compromised database.

SECOND: In view of the aforementioned communication, the General Subdirectorate of

Data Inspection proceeded to carry out preliminary investigation actions

having knowledge of the following extremes:

1. On December 13, 2018, from the Data Inspection you can access

various news published on the websites ***URL.1, ***URL.2, ***URL.3 in which

the attack carried out by the Group ***GROUP.1 against the

servers of the VOX website and access to data of some 30,000 users.

In the news it is reported that the group ***GRUPO.1 has posted on their account

Twitter (*** ACCOUNT.1) the attack on the VOX website and the information to which it has

had access, on the other hand, VOX has also posted on its Twitter account

(***ACCOUNT.2) the existence of the attack and that it has been brought to the attention of

the State Security Forces and Bodies.

2. On December 13, 2018, from the Data Inspection it is verified

the existence of a "tweet" signed by ***ACCOUNT.1 where access is reported

to 30,000 VOX registrations and a page is published with the name and

partially anonymized surnames.

3. On December 21, 2018, information is required from VOX and from the

response received on January 15, 2019 shows:

3.1 Regarding the chronology of the events

 On December 12, 2018 at 7:30 p.m., VOX learned, through

through social networks, a computer attack on the web hosted on

an external server of the company 1&1 Internet España, S.L. (onwards

1&1) with which you have signed a treatment manager contract.

 The attack was carried out by the Group ***GRUPO.1 as published in

his Twitter account ***ACCOUNT.1

 VOX proceeded to disable the attacked equipment and transfer the

incident of security to the Spanish Agency for Data Protection, the

December 13 and to file a complaint with the Civil Guard on December 14.

december.

 VOX contacts the hosting provider company 1&1 and the entity

S21Sec specialized in security for cyber attack investigation.

 VOX states that the affected data corresponds to the database

of subscribers to party news to send the newsletter that

kept 30228 records.

 On December 14 at 8:36 p.m., all its members were informed of a

message indicating the attack suffered on the web.

 VOX states that they are not aware of the use by third parties of

the data stolen in the cyberattack.

3.2 Regarding the category of data affected

 VOX states that “The data stolen by the pirates is data from the

treatment of subscribers to the notifications of the party, they are not data of

special protection, it is a simply general informative treatment of

the activities and agenda of the party, which does not imply or affiliation

political or ideological (...) is simply a treatment for sending

an informative newsletter for interested parties”

 In the Document of Registration of Processing Activities, regarding the

data processing for sending the newsletter, appears in the section

"Data category" and subsection "Identifying data" the name and

surnames, postal or electronic address and telephone. And in the subsection of

“Sensitive data” “Does not exist”.

 In the Risk Analysis document, section “Identification of the

processing of personal data", regarding the processing for sending

of newsletter, appears as BASIC Category.

3.3 Regarding the actions taken to minimize the incidence

 Disabling the form where the data is collected for the

newsletter subscribers.

In this regard, on December 13, 2018, from the Inspection

Data has accessed the VOX website at the address ***URL.4

verifying that the message appears in the subscription option

"Subscriptions in maintenance operation" without requesting any data

staff.

 Delete all data from the attacked database.

3.4 Regarding the audit report on the web object of the attack

[…]

3.5 Regarding the incident report

VOX has sent this Agency a report made by the company S21Sec

contracted to analyze the causes of the security incident.

From this report it follows:

[…]

3.6 Regarding the final resolution of the incident

[…]

THIRD: On September 25, 2019, the Director of the Spanish Agency

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

alleged infringement of article 32.1 of the RGPD typified as a serious infringement in the

Article 73 f) of the LOPDGDD and in Article 83.4 of the RGPD.

FOURTH: Having been notified of the aforementioned initiation agreement, the respondent submitted a written

pleadings in which, in summary, it stated that:

VOX has a system that we can categorize as safe

especially for the use to which it is dedicated and that the attack suffered could not

having been detected until its execution or publication on social networks.

S21Sec which did find several vulnerabilities, but could not

secure one hundred percent the tools used by the attackers, since the

They themselves are computer terrorists who use refined techniques.

Based on the recommendations of S21Sec we send a report to the Agency

of all the measures implemented in our information system to

improve security in terms of:

[…]

The subscribers of the newsletter cannot be considered ideological data. The

criterion maintained by the AEPD until now contradicts said consideration, such

As evidenced in the Reports of January 24, 2001, December 28,

February 2003, and April 29, 2008, among others. The possibility of

that people who have accessed the news subscription form

could merely be people interested in the activities of the VOX party,

without the imperative need to be affiliated with it, for which it could

The fact that said data reflected an ideological ascription would be distorted.

In other procedures dealing with similar events, the AEPD has

proceeded to file the proceedings. In this case, VOX acted

diligently and with total speed to lessen the unfavorable effects on the

rights of those affected.

FIFTH: On 12/12/2019, the instructor of the procedure agreed to open

a period of evidence practice, taking into account the actions

investigation, E/10207/2018, as well as the allegations and documents

of the investigated.

SIXTH: On February 3, 2020, by the Instructor of the procedure,

formulated a resolution proposal in the sense that by the Director of the Agency

The Spanish Data Protection Agency sanctioned VOX ESPAÑA, with NIF G86867108,

with WARNING for the infringement of article 32 of the RGPD, typified as

serious infraction in article 73 f) of the LOPDGDD.

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

documentation in the file, the following have been accredited:

PROVEN FACTS

ONE.- On 12/13/2018, from the Data Inspection there is access to various

news published on the websites ***URL.1, ***URL.2, ***URL.3 in which it is

manifest the attack carried out by the Group ***GRUPO.1 to the servers of the page

VOX website and access to data of some 30,000 users.

In the news it is reported that the La Nueve group has posted on its Twitter account

(***ACCOUNT.1) the attack on the VOX website and the information to which it has had access,

On the other hand, VOX has also published on its Twitter account (***ACCOUNT.2) the

existence of the attack and that it has been brought to the attention of the Forces and Bodies

of State Security.

TWO.- On 12/13/2018, the Data Inspection verified the

existence of a "tweet" signed by ***ACCOUNT.1 where access to

30,000 VOX registrations and a page with the name and surname data is published

partially anonymized.

THREE.- VOX proceeded to disable the attacked equipment and report the incident

to the AEPD, on 12/13/2018 and to file a complaint with the Civil Guard on

December 14th.

FOUR.- On 12/14/2018 at 8:36 p.m., a message was communicated to all its members

indicating the attack suffered on the web.

FIVE.- In the S21Sec Report that VOX commissioned to analyze the causes that

caused the security incident, the following is indicated:

A basic automated security scan has been done and 22

vulnerabilities in total, being 1 of a serious nature and 2 of a medium nature, which have

been forwarded to their managers for correction.

• A basic analysis of the source code of the server application has been carried out,

finding several serious confirmed vulnerabilities that need to be fixed and

that in general have to do with the validation of input parameters, and that

must be corrected as soon as possible.

• Some security deficiencies have been detected, which are included in the

section of recommendations, and which are considered particularly important

articulate as soon as possible, since the server's profile is considered high risk.

One of the vulnerabilities that has been ruled serious “could allow a

attacker recover username and password by intercepting an existing connection”.

The report describes the vulnerability as “application does not check parameters

of entry and can be used to infect users and for session theft”.

•S21Sec concludes that, although it has not been possible to guarantee one hundred percent the

tools used by the attackers, consider that it could have been a

SQL injection via system vulnerabilities and possible directory access

of the old web server in which backups of the web could have been dumped with

data to which the attackers had access.

•S21Sec recommends a series of technical measures and perform an analysis in

depth of the web since it considers that it will continue to be the target of campaigns

hacking and espionage.

SIX.- On 06/13/2019, VOX provides a document containing the measures

adopted in the wake of the S21Sec report.

SEVEN.- On 10/12/2019, VOX presented two reports from the HADOQ entities

IT, S.L, and SERVYTEC NETWORKS, S.L., which show that they have

the detected vulnerabilities have been solved and an optimal level of

security.

FOUNDATIONS OF LAW

Yo

The Director of the Agency is competent to resolve this procedure.

Spanish Data Protection, in accordance with the provisions of art. 58.2 of the

RGPD and in the art. 47 and 48.1 of LOPDGDD.

II

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 said data.

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 it to the competent control authority in accordance with

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.

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

Spanish Agency for Data Protection, the day after the violation occurred

of personal data, complying with the provisions of article 33.1 of the

GDPR.

Article 32 of the RGPD establishes the following:

III

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

of the 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. (The underlining is from the Spanish Agency for

Data Protection.)

From the actions carried out, it has been verified that the security measures

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

treatment, were not adequate at the time of the data breach,

because, according to the report provided (...) several serious vulnerabilities were found

confirmed that they must be corrected and that in general have to do with the

validation of the input parameters, and that they must be corrected as soon as possible.

brevity.(…)

The consequence of this lack of adequate security measures was the

public exposure on the internet of the personal data of subscribers for the

receipt of information related to the activity of the person in charge. That is, the

affected have been deprived of control over their personal data.

IV

Article 28 of the LOPDGDD establishes the following:

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 offenses. (...) (The underlining is from the Agency

Spanish Data Protection.)

v

Recitals 51 and 75 of the RGPD establish the following:

(51)

Special protection deserves personal data that, due to its

nature, are particularly sensitive in relation to the rights and freedoms

fundamental, since the context of your treatment could entail important

risks to fundamental rights and freedoms.

(75) The risks to the rights and freedoms of natural persons, of

variable severity and probability, may be due to the processing of data that

could cause physical, material or immaterial damages, in particular

(...) in cases where the treatment may give rise to problems of

discrimination, identity theft or fraud; in cases where it is deprived

interested parties of their rights and freedoms or are prevented from exercising control over

your personal information; in cases where the personal data processed reveal the

ethnic or racial origin, political opinions, (...) Emphasis is from the Agency

Spanish Data Protection.

Contrary to what VOX indicates in its allegations made to the agreement

from the beginning, this Agency is not considering the personal data subject to

the security breach, as ideological data that deserves to be subsumed under the

art umbrella 9 of the RGPD that under the heading "Special categories of data",

includes as such personal data that reveal (...), political opinions (...), but

than the type of data that has been exposed and the specific type of

exposure, that is, on the internet, a certain risk is revealed that there is

to take into account, as indicated below.

The data in question deals with the subscription to a newsletter of the

activity of the political party, and that, although it does not necessarily imply data of

ideological character, public exposure through the Internet of this information,

can lead to the realization of certain combinations with other

information - also published on the internet or by other sources, such as comments

in social networks, participation in forums, monitoring of certain profiles of

user in social networks, etc., - and place their holders in a certain

position in that sense.

On the possibility of combining information referring to a holder of

personal data, Opinion 4/2007 of the Working Group can be brought up

of Article 29, “On the concept of personal data” that although it analyzes the

possibilities of identifying someone through combinations with other

information, are very clear, when we refer to the risk of attributing

a certain political ideology, based solely on the data of a subscriber

to the information of said party, and combining it with another.

Specifically, it indicates the following: (...) when we speak of "indirectly"

identified or identifiable, we are referring in general to the phenomenon of

"unique combinations", be they small or large. In cases where,

At first glance, the available identifiers do not allow a person to be singled out

determined, it can still be "identifiable", because that combined information

with other data (whether the data controller is aware of them

as if not) will allow to distinguish that person from others. This is where the Directive

refers to "one or more specific elements, characteristic of their physical identity,

physiological, psychic, economic, cultural or social. Some of those features

are so unique that they allow effortless identification of a person (the "current

President of the Government of Spain»),

but a combination of details

belonging to different categories (age, regional origin, etc.) can also be

quite conclusive in some circumstances, especially if you have access to

additional information of a certain type. This phenomenon has been studied

widely by statisticians, always ready to avoid any

breach of confidentiality (...) Thus, the different pieces that

make up the personality of the individual in order to attribute certain

decisions.(…)

As indicated above, in this case the internet search,

for example, the name, surnames or email address of any of the

affected can offer results that, combining them with the subscription to

receive news about the activity of the political party, that is, those who have been

of the security breach, reveal to us, a certain political ideology, whose

disclosure does not have to have been consented by its owner.

This possibility represents a risk that must be assessed when treating

certain data with this characteristic and that increases the requirement of the degree of

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

confidentiality of these data.

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

function of the same to establish the measures that would have prevented the loss of control

of the data by the data controller and, therefore, by the data controllers.

holders of the data that provided them to it.

SAW

Article 71 of the LOPDGDD establishes, under the heading "Infringements"

following: Violations constitute the acts and conducts referred to in the

sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that

are contrary to this organic law.

It establishes article 73 of the LOPDGDD, under the heading "Infringements

considered serious" the following: Based on the provisions of 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 mentioned articles

in that and, in particular, 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 referred to above.

7th

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

Public, in Chapter III on the "Principles of the power to sanction", in the

Article 28 under the heading "Responsibility", the following:

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

natural and legal persons administratively, as well as, when a Law

recognize capacity to act, affected groups, unions and entities without

legal personality and independent or autonomous estates, which result

responsible for them by way of fraud or negligence

Regarding the subjective element in the commission of the violation of article

32.1 of the RGPD, it must be taken into account that VOX did not have the measures of

adequate security in order to avoid the security violation that occurred, proof of

This is, first of all, the meaning of the first report of the security incident where

It is noted that several confirmed serious vulnerabilities were found that should be

be corrected and that in general have to do with the validation of the parameters of

input, and as can be deduced from the report provided, they must be corrected as soon as possible.

brevity, and secondly, the actions that are recommended to be taken and the

which they affirm were adopted in their brief of June 13, 2019.

This lack of diligence in implementing security measures

are the element of culpability required by any imposition of

sanction.

Regarding the possible causes that caused the security violation, in the

The report of the entity S21Sec stated the following: […]

Regarding computer attacks through techniques such as injection

SQL, this Agency has pronounced itself in other resolutions, please cite by way of

example the relapse in Sanctioning Procedure No. PS/00187/2017, where

it stated the following:

(…)The intruder used a technique called “SQL Injection” to

gain access to the Planet Vtech system environment hosted on the Amazon service

Web Services. SQL injection is a type of attack known at least since

2003. Has been on the list1 of the 10 most used vulnerabilities between the years

2003 and 2011 and has affected hundreds of thousands2 of websites around the world to

despite the fact that its solution is known and simple to implement.(...)

(…) There are vulnerabilities associated with SQL injection techniques

documented since 20023. According to the OWASP14 classification, attacks

based on this type of techniques have been among the 10 most relevant since 20044.

(…)

Likewise, the lack of consideration of the risk that the

unauthorized access by third parties to data of subscribers of related information

with a political party, and its subsequent public dissemination, aggravates the guilty reproach

and sanctioning the conduct carried out by VOX.

From what has been indicated so far, the lack of diligence of VOX in the

time to implement security measures Taking into account the state of the

technique, the costs of application, 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 natural persons (art. 32 RGPD), which gives content to the element

culpabilistic of the typical and unlawful action.

viii

Article 58.2 of the RGPD establishes the following:

2. Each supervisory authority will have all of the following powers

corrections listed below:

(…)

1 http://cwe.mitre.org/top25

2 https://www.netsparker.com/blog/web-security/sql-injection-vulnerability-history

3 https://www.cvedetails.com/vulnerabilities-by-types.php

4 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

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 " 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.

3. 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.

In the present case, in view of the diligence carried out by VOX regarding

regarding the communication without delay of the security violation to this Agency

Spanish Data Protection Agency, as well as the initiation of actions aimed at

minimize the negative consequences of the aforementioned security breach, and

indicated in proven facts six and seven of this resolution, which highlight

manifest that after the security incident and the reports that they commissioned to the

experts in security, the entity has solved the vulnerabilities detected and

the security level has improved, it is considered in accordance with the law not to impose a sanction

consisting of an administrative fine and replace it with the sanction of a warning of

in accordance with article 76.3 of the LOPDGDD in relation to article 58.2 b) of the

GDPR.

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 VOX ESPAÑA, with NIF G86867108, for an infringement of the

Article 32 of the RGPD, typified in Article 83.4 of the RGPD, a sanction of

warning.

SECOND: NOTIFY this resolution to VOX ESPAÑA.

In accordance with the provisions of article 50 of the LOPDGDD, the

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 period of

month 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, the firm resolution may be provisionally suspended in administrative proceedings if the interested party expresses his intention to file a contentious appeal-administrative. If this is the case, the interested party must formally communicate this made by writing to the Spanish Agency for Data Protection, introducing him to the agency [https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. Also must transfer to the Agency the documentation that proves the effective filing of the contentious-administrative appeal. If the Agency were not aware of the filing of the contentious-administrative appeal within two months from the day following the notification of this resolution, it would end the precautionary suspension.

Electronic Registration of through the Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es