 Procedure No.: PS/00117/2020

938-300320

RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following

BACKGROUND

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

initial notification sent by VTS MEDIA, S.L. in which they inform this Agency

about the detection of a security breach on 10/24/2019, related to the

exposure on the Internet of technical logs (records of server activity), in

which initially did not appreciate that there was personal information. Indicate that

subsequently, on 11/3/2019, the message appears in a media outlet

exposure of personal information of users, and thoroughly investigated the

logs personal information is detected.

SECOND: In view of the aforementioned security breach notification, the Subdirectorate

General Data Inspection proceeded to carry out preliminary actions of

investigation having knowledge of the following extremes:

BACKGROUND

Security breach notification date: November 5, 2019.

INVESTIGATED ENTITIES

VTS MEDIA, S.L. (hereinafter VTS), with NIF B63546253 and with address at c/ Doctor

Trueta 183, Floor 8, Pta. 1, 08021 Barcelona.

RESULT OF THE INVESTIGATION ACTIONS

1.- FACTS

Manifestations:

VTS states in the notification of the security breach that "due to a

failure in the log servers (based on Elasticsearch) a service was contracted

External storm between May 24, 2019 and October 25, 2019

consisting of three external cloud servers. On these servers a new

cloud without any historical data, but on September 5 the logs were copied

generated in this period of time to a new cluster that was discovered by

this error in the interpretation of the documentation, specifically, a functioning

inadequate firewall which allowed the connection to our Elasticsearch without

need to use credentials and see the corresponding logs".

They indicate in this initial notification that the number of affected has been about 300,000

with basic data, IP addresses, contact data and ID of its users.

In a second data expansion notification about the security breach

increase the number of affected users to 550,000, and include in the typology of

data access credentials or identification.

Regarding customer payment method data, they indicate that it only comes from their

payment provider part of the users' credit card numbering.

They provide a copy of the log file where they indicate said circumstance.

They also provide in this second notification a report called "MEASURES OF

VTSMEDIA SECURITY" where they reflect the inquiries about the possible causes

of the occurrence of the gap in a description and chronology of the facts, the detail

of the exposed data and the security measures both present and

implemented after the security breach.

Description of the facts:

 In the report on “VTSMEDIA SECURITY MEASURES” provided by the entity

a description of facts is made, indicating that they used an indexing

“ElasticSearch” log saver to save technical logs and that due to a failure

in "ElasticSearch" decided to install a new cluster (group of servers) in

a “Scaleway” cloud provider

They state that the system was installed following the official documentation, and the

protection was done using a firewall (firewall) so that access

only possible from the IP addresses of the entity.

 They also state that their procedures to implement the decree did not fail.

security, since they have managed to determine in the internal investigation

that the protection rules that configure the firewall were created and applied correctly.

correctly (they attach a proof of eGuarantor, indicating that they have followed the

recommendation of the website of the Civil Guard) in which they indicate that

to see that the firewall protection rules were created on 05/27/2019.

They indicate that they have reviewed history of failures in the company "Scaleway" and have

found user reports with similar problems in the past with res-

Regarding the firewall and the control panel. On 05/29/2019 (2 days later) this

company reports an incident on the operation of its panel, for a

alleged API instability.

They state that they have requested the logs referring to these operations from the company.

prisoner, receiving as an answer that they have been deleted and that they no longer have

nene of that information.

 They state that they did not detect this anomaly since they could normally enter

you from your private network. None of their technicians checked if the firewall rules

they were being applied.

 They also provide a detailed chronology of the events that is summarized below.

continuation:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/15

05-24-2019: Due to a failure in the Elasticsearch cluster, containing

internal technical logs, new servers were hired from a provider

external temporarily. They were configured in the provider “Scaleway.com”

firewall rules.

10-24-2019: Members of the user support team receive a ticket (co-

incidence communication) from an external person who claims to have found

a vulnerability in the entity's infrastructure.

- Customer service asks for more details.

- They receive at 19:16 (Spanish local time) the response from the researcher where

reports the IP, Port and type of instance (elasticsearch) exposed.

- The person who attended the ticket without knowing the seriousness, left it pending

to be able to consult it with a technician who was no longer working hours, he

ends at 6:30 p.m.

10-25-2019:

- At 10:00 a technician reviews the data provided on the ticket.

- Verifies that the service was indeed exposed because the fi-

firewall were not being applied despite having been created, configured and

applied in the scaleway service.

- Proceed to stop the service and eliminate the temporary Cluster that was still

active.

- The technical person did not know the content or scope of that Cluster.

- Transfer a response to "customer service" to respond to the ticket.

- The person confirms the resolution of the incident.

03-11-2019:

- At 7:10 p.m. a member of the company receives a press release and understands it.

part with the entire technical team CTO, DPO and the person in charge of infrastructure,

noticing that it is related to the removed elasticsearch cluster.

- Technical investigations are initiated in reference to the possible content exposed.

to from elasticsearch cluster removed.

- A first internal investigation is carried out to assess the scope of the incident.

dence. User data is discovered and investigations are launched.

04-11-2019:

- The entire technical team carries out a first assessment, finding two

indexes with personal customer data. After a day investigating, he con-

tance of the user data found.

- The initial statement is published.

- A notice is added to the header of the website linking to the statement that follows-

was active as of the report date 11/12/2019.

- Publication on social networks linking to the statement.

- Emails are sent with the informative note and link to the communication.

do to affected users.

- Measures are prepared to avoid future similar events.

- Tasks derived from the aforementioned measures are started.

- We attend to the media that contact us to request more information.

mation.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

05-11-2019:

- At 00:39 the report is sent to the AEPD.

- Requests for information or deletion of users are attended.

06-11-2019:

- The technical team continues to thoroughly review the logs (145 million records)

tros) and find new user data.

- They realize that there are processes that delete the logs of sending emails to the

30 days.

- For the above reason, it is decided to consider all users with e-mail affected.

validated email.

- First contact with INCIBE.

07-11-2019:

- The investigation is concluded and the number of affected and

exposed data.

- It is decided to apply a preventive password renewal policy to certain

affected users.

08-11-2019:

- A new communication is made to the users.

- The change of password is forced to about 2000 users.

09-11-2019: Investigations continue to confirm that there are no more

exposed data

11-11-2019: The information in the public statement is expanded with more detail.

lles.

The entity has provided a copy of the communications sent to users.

About the exposed data:

They report that the total records in the Elasticsearch Cluster generated during the

period 05/24/2019 until 09/04/2019 and exposed until 10/25/2019 is

141,545,213 records.

In all the records, the passwords appear encrypted, except for some that indicate

they correspond to an intentional “debug” that was not eliminated so they remain

exposed 7,526 occurrences out of a total of 1,757 unique affected users.

Users' bank card numbers appear truncated. Indicate that

With these data it is impossible to carry out any operation or purchase.

The identification numbers correspond to identity documents of different

countries, in the case of Spain, mostly DNI and NIE. Only the number appears

the name is not specified, nor does it contain the image, nor the type of document

nor more information in relation to said document, of a total of 1915 unique users

affected.

Other data corresponds to the detail necessary to withdraw donations

and prizes won on the web, with a total of 897 records with personal data:

of 697 unique Headlines, 527 unique Telephones and 663 unique postal addresses (without

include city, province or country). A total of 28,767 unique registrations with telephones belonging to 2,657 unique users affected by the telephone number.

In all the action logs, the IP from where the action was executed is added with an approximate number of records due to the technical complexity to extract this information, about 9,170,853 records. The number of unique IPs is 759,806 corresponding to a total of 215,878 unique users affected by the exposure of your IP.

The approximate number of records with readable email address due to the technical complexity to extract this information is 50,000,000. Number approximate number of unique emails in those records: 330,000, which corresponds to the Approximate number of unique users affected by said data.

During chats (or conversations) between sender and users, a record of the conversations. The total number of records with exposed conversations is 1,502,933 corresponding to 8,964 unique users with conversations. in the logs the clear message (text) and the user's IP appear.

These are video servers of a sexual nature such as “***SERVIDOR.1” or “***SERVER.2”.

They have provided extracts from the logs where the structure of the data can be seen exposed. They show that the exposed information of the accounts of the broadcasters (people who broadcast the videos with sexual content also commonly referred to as Camgirls) consists of at least your first and last name, phone number and full mailing address.

They indicate that they have carried out cyberintelligence investigations in collaboration with the INCIBE and both they and INCIBE have not detected that the logs have been leaked or that are available to third parties on any Internet site, following performing this detection routine weekly.

They state that INCIBE expressly congratulated them for the management and collaboration made with them. They attach an email that INCIBE sent on the 28th of November at 4:05 p.m. where it is stated that they did not detect subsequent uses of the data or filtration on the Internet and congratulations for the management and collaboration.

2.- PRE-EXISTING MEASURES

The entity has provided a copy of the Record of Treatment Activities (RAT) of the which is responsible, dated 02/22/2019. It has also provided a copy of a Risk Analysis version 1.1, although it is dated 11/14/2019

As indicated, when making the change to "Scaleway" in the firewall, they were created and firewall configuration rules were applied, providing the entity with several screen impressions certified by eGuarante dated 9/11/2019 in which They see three rules applied to incoming traffic on the servers.

In another screen it is read that on 05/27/2019 there are no reported incidents and that in date 05/29/2019 instability is detected.

Regarding the prior diligence in contracting the Scaleway service, the representatives of the entity state that at the time of choosing said provider of services was taken into account:

1- Which is one of the largest server providers in France (formerly known as Online.net).

2- It has ISO 27001 and 50001 certifications as well as HDS.

3- Its datacenters are TIER III (classification according to ANSI/TIA-942 standard) and are

located in ***COUNTRY.1

4- The privacy policy was audited and determined in accordance with the requirements of the

data protection regulations, where a separate section is contemplated in the case

of security breaches.

They indicate that the privacy policy itself, which must necessarily be accepted to

contract with Scaleway, includes all the elements included in article 28.3 of the

RGPD with regard to the content of the contract between the person in charge and the person in charge.

All of the above led to the internal conclusion that it was an optimal choice for

technical and security needs, but also legal ones.

3.- MEASURES SUBSEQUENT TO THE SECURITY BREACH

The representatives of the entity have stated that they are carrying out

modifications to the measures after the fact, detailing the

following:

-

The hiring of the CISO (Chief Information Security Officer) is carried out for the day

11/11/2019.

- Improve communication between providers of this type of service.

-

-

-

-

-

Determine list of logs with data not necessary for technical review and eliminate

nar those particular logs.

Encryption of the entire content of the logs.

Review of log deletion policy and reduce times as far as possible.

possible.

Recryption of data with new keys and application of hash algorithms to the

passwords.

Additional review of all systems with storage of any type of

data, to eliminate unnecessary data or encrypt the corresponding

Additionally, they detail a series of security measures aimed at detecting

and management of vulnerabilities based on DevSecOps methodologies (methodology of

work that integrates security into software development and operation). I know

include, among other measures, the use of tools for automatic analysis

of the web environment imitating an external malicious agent, periodic audits and

reviews of all incidents by a security analyst.

To minimize the adverse effects of the security breach, the entity

performed the following actions:

03-11-20193

Review of the state of the machine where the data was exposed and verification

tion of its off.

First analysis of the exposed data.

The bug that prevented receiving emails to the privacy email from outside has been fixed

of the company.

04-11-2019

The technical team performs a first assessment, finding two indices with data

personal cough.

The technical team records that it has not found other user data.

The initial statement is published.

A notice is added on the web linking to the statement.

Publication on social networks linking to the statement.

Emails with the informative note and link to the communication are sent to

affected users, differentiating between less sensitive data (emails and

IP's) of the most sensitive (documentation and postal address).

Measures are being prepared to avoid future similar events.

Tasks derived from the aforementioned measures are initiated, including reviewing the

Curation of all system services (access to machines and international networks)

nas above all).

They attend to the media that contact them to request more information.

05-11-2019

The report is sent to the AEPD.

Requests for event information and/or data deletion are answered.

The technical team continues with the tasks arising from the previous point.

06-11-2019

The technical team performs another more exhaustive review. They become aware of the existence

ence of another index within the technical logs with more exposed user data.

They find that there is a lack of available data that could have been exposed due to

that some indices are automatically deleted after a month and others after

3.

07-11-2019

C/ Jorge Juan, 6

28001 – Madrid

The infrastructure team retrieves the backup of the used deleted indexes

to fill in the history of the new Cluster.

In the revision carried out on these new data, new personal data are found.

nals and the total numbers affected.

It is decided to develop a password renewal policy for users

affected with prior notice.

It is decided to rectify the public statement.

Collaborate with INCIBE and send the complete report to INCIBE

08-11-2019

The aforementioned forced password change is applied to the affected users

in the previous point 3.

11-11-2019 The new public statement is published with the changes that have arisen.

THIRD: On June 17, 2020, the Director of the Spanish Agency for

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

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

FOURTH: On 07/1/2020 and entry registration 022543/2020, VTS presented

allegations to the initiation agreement in the sense that it does not want to make any

manifestation in this regard, remaining at the disposal of this AEPD to collaborate in

everything that is necessary. Consequently, pursuant to the provisions of articles

64.2.f) and 85 of Law 39/2015, of October 1, on Administrative Procedure

Common to Public Administrations, the start-up agreement can be considered

resolution proposal. Consequently, this Agency proceeds to issue a Resolution.

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

of Data in this procedure the following are considered proven facts,

PROVEN FACTS

FIRST: dated 10/24/2019 VTS, as data controller,

exposed on the internet personal information of its clients collected during the period

From May to October. The security breach was confirmed on 11/3/2019 after the

investigations initiated and the publication of the news in a media outlet.

SECOND: On 11/5/2019, VTS notified this Agency of a breach of

security as a consequence of the exposure on the Internet of technical logs (records

of activity of the servers) in which they were embedded and technically

difficult to access personal data of customers.

THIRD: The affected data categories are IP addresses, DNI, addresses of

email with passwords, truncated card numbers and customer chats.

FIFTH: On 9/11/2019, the security of the information system is restored

of VTS.

FOUNDATIONS OF LAW

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

control, 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

resolve this procedure.

Yo

The defendant is charged with the commission of an infraction for violation of Article 32

of the RGPD, which indicates that “transcription”. The infraction is typified in Article 83.4

of the RGPD and is classified as Serious in article 73.f) of the 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”.

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.

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

Spanish Data Protection Agency, the day after the data breach occurred

personal, in compliance with the provisions of article 33.1 of the RGPD.

Article 32 of the RGPD establishes the following:

IV

"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.)

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 offenses. (...)" (The underlining is from the Agency Spanish Data Protection.)

Recitals 51 and 75 of the RGPD establish the following:

SAW

"(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, financial loss, reputational damage,

loss of confidentiality of data subject to professional secrecy, reversal not

authorized pseudonymization or any other economic or social damage

significant; 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

politics, religion or philosophical beliefs, trade union membership and treatment

of genetic data, data relating to health or data on sexual life, or the

criminal convictions and offenses or related security measures; in cases where

those that evaluate personal aspects, in particular the analysis or prediction of

aspects related to performance at work, economic situation, health,

personal preferences or interests, reliability or behavior, situation or

movements, in order to create or use personal profiles; in cases where

personal data of vulnerable persons, in particular children, are processed; or in the

cases in which the treatment involves a large amount of personal data and

affects a large number of stakeholders., (...)”

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

that VTS had in relation to the data that it submitted to treatment as

responsible, were not adequate at the time of the breach of

security, since according to the report provided “(…) several vulnerabilities were found

serious confirmed that 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 security measures, both technical and

appropriate organizational measures was the public exposure on the internet of personal data

of subscribers to receive information related to the activity of the

responsible. In other words, those affected have been deprived of control over their

personal information.

Another consideration is that the data processing to which those affected are subscribed,

refers to the activity defined in art 9 of the RGPD as special categories of

personal information.

On the possibility of combining information referring to a data owner

personal data, Opinion 4/2007 of the Working Group of the

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 sexual behavior, based solely on the data of a subscriber

and combining it with others.

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 (…). So the different pieces come together.
that make up the personality of the individual in order to attribute certain
decisions. (…)"

As stated above, searching the internet for, for example, the name,
surnames or email address of any of those affected can offer
results that combining them with the content of the exposed logs of the clients,
could reveal a certain behavior and sexual life, and that it does not have to
have been consented by its owner.

This possibility supposes an added risk that has to be assessed beforehand and that
increases the demand for the degree of protection in relation to safety and
safeguarding the rights and freedoms of those affected, by virtue of the provisions of
the aforementioned article 9 of the RGPD.

This risk and the impact on the rights and freedoms of those affected must be

taken into account by the data controller and, based on it,

establish the technical and organizational measures that prevent the loss of

control of the data by the data controller and, therefore, also by

the holders of the data that provided them.

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 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 result

appropriate to guarantee a level of security appropriate to the risk of the treatment,

in the terms required by article 32.1 of Regulation (EU) 2016/679."

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

LOPDGDD referred to above.

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

Chapter III on the "Principles of the power to impose penalties", in article 28

under the heading “Responsibility”, the following:

viii

"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.”

This lack of diligence in implementing adequate security measures

of a technical and organizational nature constitute the element of sufficient culpability

which requires the imposition of a penalty.

Likewise, the lack of consideration of the risk that access may entail does not

authorized by third parties to data of subscribers of information related to the

contracted service, and its subsequent public dissemination, aggravates the guilty reproach and

sanctioning the conduct carried out by VTS.

Article 58.2 of the RGPD establishes the following:

IX

"two. 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", 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

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."

data.

X

In the present case, in view of the diligence carried out by VTS in relation to

to the notification without undue delay of the security breach to this Agency

Spanish Data Protection Agency, diligent and reiterated communication by various

means to those affected, the technical complexity of the information systems, the beginning

diligent and prompt action aimed at minimizing the negative consequences of

the security breach, no recurrence, that the security breach had its

origin in a security flaw occurred in the new service provider

Scaleway having verified that VTS had the appropriate measures

certified security (TIER III, according to ANSI/TIA 942 standard) installed by

defect, allows to consider a reduction of guilt in the imputed facts, for

what is considered in accordance with the law not to impose a sanction consisting of a fine

and replace it with the sanction of warning in accordance with the

article 76.3 of the LOPDGDD in relation to article 58.2 b) of the RGPD.

Therefore, in accordance with the applicable legislation and assessed guilt in the

imputed facts whose existence has been proven, the Director of the Agency

Spanish Data Protection RESOLVES:

FIRST: IMPOSE VTS MEDIA S.L., with NIF B63546253, for an infringement of the

Article 32 of the RGPD, typified in Article 83.4 of the RGPD and 73.f) of the LOPDGDD,

a warning sanction.

SECOND: Require VTS MEDIA S.L. so that within three months it contributes to

this AEPD the following documentation:

 Provide a regulated procedure for action in the event of a security incident

computer that allows knowing if it has affected personal data and that

identify affected locations and resources (security breach).

 Provide audit, which should include risk analysis and evaluation of

impact in accordance with the provisions of article 35 of the RGPD, carried out after the

security breach that certifies the correct operation and configuration

of the information system in order to avoid future incidents such as the

analyzed in this procedure. This audit should also

be made and remain available to the AEPD when they occur

modifications in the resources or treatments that affect personal data.

THIRD: NOTIFY this resolution to VTS MEDIA S.L., with NIF

B63546253, and address at c/ Doctor Trueba 183, 8th Floor, Door 1, 08021 Barcelona.

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