Procedure No.: PS/00237/2019

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: A.A.A. (hereinafter, the claimant) dated July 17, 2018

filed a claim with the Spanish Data Protection Agency. The

claim is directed against XFERA MÓVILES, S.A. (YOIGO) with NIF A82528548 (in

later, the claimed one). The grounds on which the claim is based are that from the

06/08/2018, receives SMS from Yoigo addressed to a third party and that when entering the Yoigo website

Yoigo your phone number and a password that was sent to you by SMS, you can access the

data of said third party.

The claimant has made the facts known to the entity in several

times, but the issue remains unresolved.

Along with this claim, a screenshot of SMS received, a screenshot of

of the conversation held by e-mail with the third party, as well as a screenshot of the

data of said third party to which he had access through the web.

SECOND: Upon receipt of the claim, the Subdirectorate General for Inspection of

Data proceeded to carry out the following actions:

On September 26, 2018, the claim with

reference E/5795/2018, submitted for analysis and communication to the complainant of the

decision made in this regard. Likewise, he was required so that within a month

send certain information to the Agency:

- Copy of the communications, of the adopted decision that has sent the claimant to

purpose of transferring this claim, and proof that the claimant has received

communication of that decision.

- Report on the causes that have motivated the incidence that has originated the

claim.

- Report on the measures adopted to prevent similar incidents from occurring.

- Any other that you consider relevant.

On September 26, 2018, the claimant was informed of the receipt of the

claim and its transfer to the claimed entity.

On November 29, 2018, the respondent entity requested an extension

deadline to respond to the transfer.

On February 13, 2019, without having received a response from the operator,

The claim is accepted for processing.

On February 25, 2019, a request for information was sent to

said entity on the facts denounced, stating its receipt that same day.

THIRD: On July 2, 2019, 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: Despite having been notified of the aforementioned initial agreement on 07/14/2019, the

Respondent has not submitted a pleadings brief.

FIFTH: On August 28, 2019, the instructor of the procedure agreed to the

opening of a period of practice tests, considering incorporated the

previous investigative actions, E/01816/2019, as well as the documents

provided by the claimant.

SIXTH: On September 3, 2019, a resolution proposal was formulated,

proposing that the defendant be punished for an infraction of article 32 of the

RGPD, typified in article 83.4 of the RGPD, with a fine of €60,000.00

(SIXTY THOUSAND euros).

SEVENTH: On September 17, 2019, the respondent requests a copy of the

proceedings. This referral is processed by the AEPD, on October 3, 2019 by

certified mail, since the requested copy of the file has a size that

exceeds the maximum allowed in the Notific@ system, used by the organs of the

Administration for the electronic practice of your notifications.

PROVEN FACTS

On June 8, 2018, the claimant receives SMS from the respondent addressed to

a third party and that when you enter your telephone number and a password on the website of this entity

that was sent to you by SMS, you can access the data of said third party.

The claimant has made the facts known to the entity in several

times, but the issue remains unresolved.

A screenshot of the SMS received, a screenshot of the conversation is provided

maintained by e-mail with the third party, as well as a screenshot of the data of said third party

to which he had access through the web.

FOUNDATIONS OF LAW

Yo

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

control authority, and as established in arts. 47 and 48.1 of the LOPDPGDD, the

Director of the Spanish Data Protection Agency is competent to resolve

this procedure.

II

The defendant is imputed the commission of an infraction for violation of the

article 32 of the RGPD, which states that

"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.

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

certification mechanism approved under article 42 may serve as an element

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

present article.

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

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

manager and has access to personal data can only process said data

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

Law of the Union or of the Member States."

III

In the present case, the claim focuses on the fact that the claimant receives SMS

of Yoigo addressed to a third party and that when entering your telephone number on the Yoigo website

and a key that was sent to you by SMS, you can access the data of said third party.

Thus, it is understood that we would be facing a presumed violation of the

article 32 of the RGPD indicated in the foundation II, since the person in charge and the

in charge of the treatment must apply technical and organizational measures

appropriate to guarantee a level of security appropriate to the risk, which in its case

includes, but is not limited to, pseudonymization and encryption of personal data, the ability to

to guarantee the confidentiality, integrity, availability and permanent resilience

treatment systems and services, the ability to restore the availability and

access to personal data quickly in the event of a physical or technical incident,

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

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

IV

In accordance with the evidence available in this

time, and without prejudice to what results from the investigation, it is considered that the

Known facts could constitute an infraction, attributable to the defendant,

for an alleged violation of article 32 of the RGPD indicated in foundation II.

v

The infringement is typified in article 83.4 a) of the RGPD, which considers that the

infraction of “the obligations of the person in charge and of the person in charge in accordance with the articles

8, 11, 25 to 39, 42 and 43” is punishable, in accordance with section 4 of the aforementioned

Article 83 of the aforementioned Regulation, “with administrative fines of EUR 10,000,000

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

maximum of the overall annual total turnover of the previous financial year,

opting for the highest amount

The regulation of infractions in the LOPDGDD is more precise in terms of

the situations giving rise to an infringement and their consideration, so that it is

much easier to know the limitation period of that infraction (that is, if it is

considered mild, serious or very serious) and in view of the administrative sanction to be imposed

for its non-compliance.

The LOPDGDD in its article 71, Violations, states that: "They constitute

infractions the acts and behaviors referred to in sections 4, 5 and 6 of the

Article 83 of Regulation (EU) 2016/679, as well as those that are contrary to the

present organic law”.

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

considered serious”:

“Based on the provisions of article 83.4 of Regulation (EU) 2016/679

are considered serious and will prescribe after two years the infractions that suppose a

substantial violation of the articles mentioned therein and, in particular, the

following:

(…)

d) The lack of adoption of those technical and organizational measures that

are appropriate to effectively apply the principles of protection of

data from the design, as well as the non-integration of the necessary guarantees in the

treatment, in the terms required by article 25 of Regulation (EU) 2016/679.

e) Failure to adopt the appropriate technical and organizational measures

to ensure that, by default, only the personal data necessary to

each of the specific purposes of the treatment, as required by article

25.2 of Regulation (EU) 2016/679.

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.

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

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

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

SAW

In accordance with the provisions of the RGPD in its art. 83.2, when deciding to impose

an administrative fine and its amount in each individual case shall be taken into account

aggravating and mitigating factors that are listed in the aforementioned article, as well as

any other that may be applicable to the circumstances of the case.

Consequently, the following have been taken into account as aggravating factors:

□

□

unintentional negligent action, but on significant data that allows the

identification of a person (article 83.2 b)

affect basic personal identifying data (name, a number of

identification, the line identifier), according to article 83.2 g)

7th

On the other hand, article 83.7 of the RGPD provides that, without prejudice to the

corrective powers of the control authorities under art. 58, paragraph 2,

each Member State may lay down rules on whether and to what extent

impose administrative fines on authorities and public bodies established in

that Member State.

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 XFERA MÓVILES, S.A. (YOIGO), with NIF A82528548, by

an infringement of article 32 of the RGPD, typified in article 83.4 of the RGPD, a

fine of €60,000 (sixty thousand euros).

SECOND: NOTIFY this resolution to XFERA MÓVILES, S.A. (YOIGO).

THIRD: Warn the sanctioned party that he must make the imposed sanction effective once

Once this resolution is enforceable, in accordance with the provisions of the

art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (hereinafter LPACAP), within the payment term

voluntary established in art. 68 of the General Collection Regulations, approved

by Royal Decree 939/2005, of July 29, in relation to art. 62 of Law 58/2003,

of December 17, through its entry, indicating the NIF of the sanctioned and the number

of procedure that appears in the heading of this document, in the account

restricted number ES00 0000 0000 0000 0000 0000, opened on behalf of the Agency

Spanish Data Protection at Banco CAIXABANK, S.A. Otherwise,

it will be collected during the executive period.

Received the notification and once executed, if the date of execution is

is between the 1st and 15th of each month, both inclusive, the term to carry out the

voluntary payment will be until the 20th day of the following month or immediately after, and if

is between the 16th and last day of each month, both inclusive, the term of the

payment will be until the 5th of the second following month or immediately after.

In accordance with the provisions of article 50 of the LOPDPGDD, 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 LOPDPGDD, 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 Electronic Registration of through the C/ Jorge Juan, 6 28001 – Madrid www.aepd.es sedeagpd.gob.es

[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.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es