 Procedure No.: PS/00298/2020

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: Ms. A.A.A. (the claimant), on 10/08/2019 filed a claim

before the Spanish Agency for Data Protection. The letter is also directed against

TELEFÓNICA MOBILES DE ESPAÑA, S.A.U. with NIF A82018474 (hereinafter, the

reclaimed). The grounds on which the claim is based are, in short: that the

O2 telephone operator has an APP to check bills or consumption,

application that, for installation, also requests access to all data

stored on the device.

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

Data Inspection proceeded to carry out the following actions:

On 11/27/2019, the claim submitted was transferred to the defendant for analysis

and he was required so that within a month he sent to the determined Agency

information:

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

claimant regarding the transfer of 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 incidents from occurring

Similar.

- Any other that you consider relevant.

On 12/13/2019, the respondent stated that the "MiO2" mobile application, intended for line management, bill consultation and customer consumption, can be used without accept the different permissions that are requested during your download; the application of those permissions are done to enrich the customer experience but they are not necessary for the basic aspects of the application. Regarding the specific permission of "Storage" is requested since it is necessary to be able to download the invoices in the terminals whose operating system of the clients is Android. So You can request the receipt of paper invoices in accordance with the regulations valid.

THIRD: On December 1, 2020, the Director of the Spanish Agency for Data Protection agreed to initiate a sanctioning procedure against the claimant, for the alleged violations of articles 5.1.c) of the RGPD, and article 13 of the RGPD, typified in article 83.5 of the RGPD.

FOURTH: On May 17, 2021, a resolution proposal was formulated, proposing that the Director of the Spanish Data Protection Agency sanction to TELEFÓNICA DE ESPAÑA, S.A.U., with NIF A82018474, for two infringements against:

Article 5.1.c) of the RGPD, typified in art. 83.5 a) GDPR with a fine

□

50,000 euros (fifty thousand euros)

Article 13 of the RGPD, typified in article 83.5 b) of the RGPD with a

fine of 50,000 euros (fifty thousand euros)

FIFTH: On May 31, 2021, arguments are presented to said proposal

of resolution by the claimed party indicating the following:

In relation to the infringement of article 5.1 c) of the RGPD, the respondent indicates that:

“It is not true that the installation of the application requires access to the

personal data stored by users on the device.

The Mi O2 mobile app can work properly without the need to

accept their different permissions, for which their express acceptance is necessary.

In addition, the 7 client is informed at all times prior to his

authentication of what each permission is needed for.

With regard to the specific permit called "Storage", which the AEPD

understood as "excessive", it is necessary to show that it would be treated

of a permission that is textually identified with the literal:

• Permission to access photos, media content and device files, but that

despite such introductory expression, it only refers to the fact that by means of the consent to

With this permission, you authorize O2 to be able to download your invoices to your device.

This permission is only requested on Android devices.

This party considers that the execution of said permission is not excessive at all, and

that is adequate, pertinent and limited to what is necessary for its purpose: the user is informed

which is only necessary to be able to download your invoices to the device.

In no case for the download of the invoice, the My O2 mobile application would treat the

data of the photos, multimedia content or files that the user has in his

device, being only the necessary permission solely and exclusively for the

Download the invoice in pdf format.

Otherwise, there would be no way for the user to download their invoice given

that this requires access to this section of the device.

As indicated in the allegations to the Initial Agreement and that we return to

reproduce given the omission of these facts in the AEPD Resolution Proposal,

this part cannot modify the literal “ACCESS PERMISSION TO PHOTOS,

MEDIA CONTENT AND FILES ON THE DEVICE”, which is displayed to users

users of the application when accepting the permission, and which serves as the basis for the

initiation of the sanctioning file by the AEPD, given that it is a text

default by Android system.

For these purposes, we refer the AEPD to the website for Android developers

https://developer.android.com/training/permissions/requesting, where following the

permissions is indicated:

Note: Your app cannot customize the dialog that appears when you call launch().

If you want to provide more information or context to the user, change your app's UI

in order to make it easier for users to understand why a function needs

a particular permit. For example, you can change the button text that enables

the function.

In addition, the text of the system permissions dialog refers to the group of

permissions associated with the permission you requested.

This way of grouping permissions is designed for ease of use of the system, and

your app should not depend on permissions inside or outside a permission group

specific.

In this sense, and following the guidelines indicated by Android, this part has tried

by explaining the permissions, both on our website and in the

Conditions of use of the application, as in the help page, really indicate

what it is needed for: “by consenting to this permission, you authorize O2 to

be able to download your invoices to your device.

This permission is only requested on Android devices.” 8

For this reason, we consider that the action actually carried out -that we remember in any

moment supposes the access to photos, multimedia contents and device files-

complies with the principle of data minimization established in art. 5.1.c) of the

RGDP, as these are treated appropriately, pertinently and limited to what is necessary.

The only purpose of the request for permission to access the device is the possibility

that the user can download their invoice.

Therefore and in conclusion, TME has not violated article 5.1.c) of the RGPD.”

Secondly, in relation to the violation of article 13 of the RGPD, the

claimed alleges in relation to the permissions requested in the mobile application what

Next:

“In clause 11 of the O2 Mobile Application Terms of Use itself,

referring exclusively to the permissions requested in the mobile application:

11. Permissions To use certain services or functionalities and depending on the

operating system of your terminal, you will need to give your prior consent to Mi

O2 to collect additional information about you or about information found

stored on your device.

This consent may be canceled or granted again at any time.

through the permissions section of your own device.

6 Specifically, Mi O2 may request the following permissions for the following

functionalities:

• Access permission through Face ID: by consenting to this permission

available only for IOS terminals, you authorize O2 to collect the information

available on your facial recognition IOS device, so you can

access the My O2 app without entering login credentials.

• Access permission by fingerprint: by consenting to this

permission available only for Android terminals, you authorize O2 to collect the

information available on your Android device of your fingerprint, so that

You will be able to access the Mi O2 application without the need to enter your login credentials.

access.

• Contact access permission: By consenting to this permission,

available for all types of devices, you authorize O2 to access your list of

contacts from your device to offer you a better experience.

In this way, the images and names of your agenda can be seen in your lines and in

the detail of the calls that appear in the application.

• Permission for consumer advertisements: by consenting to this permission,

available for all types of devices, you can view and receive consumption notices

in real time.

• Access permission to photos, media content and device files:

by consenting to this permission, you authorize O2 to be able to download the

invoices of your O2 products and services that you want on your device.

• Consumption widget activation permission: display of GB consumed

in the current cycle on the line/s that the user chooses to see.

In this sense, the AEPD cannot affirm that the mobile application consults invoices

of the client prior to its download or that affects all the data stored

on the device or data from third parties outside the entity.

The client is informed at all times in a clear, simple and transparent way and

prior to downloading the application, both the data of the person in charge of the

treatment as of the implications of the acceptance of the different permissions of the

application, without in any case its acceptance becoming mandatory for its use.

For all these reasons, TME can affirm that it complies at all times with the requirements

established in art. 13 of the RGPD without being able to be charged with a sanction for this

done."

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited:

PROVEN FACTS

FIRST: The telephone operator O2 has a computer application to

consult the invoices or consumption of its users and for the installation of said

application, access to all personal data stored by users is required.

users on the device.

SECOND: On November 27, 2019, the claim was transferred to the defendant,

responding on December 13, 2020 that the "MiO2" mobile application, intended for

line management, bill consultation and customer consumption, can be used without

accept the different permissions that are requested during your download; the application of those permissions are done to enrich the customer experience but they are not necessary for the basic aspects of the application.

THIRD: On December 30, 2020, in response to the agreement to initiate this sanctioning procedure, it is alleged by the defendant that he does not breach articles 13 and 5.1 c) of the RGPD indicated as "all users of the My O2 Mobile Application already has all the necessary information and that must be provided in accordance with art. 13 of the RGPD, since said information is included in the "Data Protection" clause of the different General Contracting Conditions of the Products and Services O2 brand, which both the AEPD, our customers, and any interested person you can consult all the time on our website www.o2online.es/informacion-legal. “

in

FOURTH: On May 31, 2021, arguments are presented to the proposal of resolution proving that it is not necessary for the installation of the application the access to personal data stored by users on the device, as well such as compliance with article 13.1 of the RGPD.

FIFTH: In the privacy policy and in the Conditions of use of the Application O2 mobile, information is given on each access permit that is requested, its purpose, the reason for that access and the possibility of granting and canceling them.

FOUNDATIONS OF LAW

Yo

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.

II

Article 5, Principles relating to processing, states that:

"1. The personal data will be:

(…)

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

that are processed ("data minimization");

(…)

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").

(…)”

III

Second, article 13 of the RGPD determines the information that must be

be provided to the interested party at the time of collecting their data, establishing the

Next:

“Article 13. Information that must be provided when personal data is

obtain from the interested party.

1. When personal data relating to him is obtained from an interested party, the

responsible for the treatment, at the time these are obtained, will provide

all the information indicated below:

a) the identity and contact details of the person in charge and, where appropriate, of their

representative;

b) the contact details of the data protection delegate, if applicable;

c) the purposes of the treatment to which the personal data is destined and the legal basis

of the treatment;

d) when the treatment is based on article 6, paragraph 1, letter f), the interests

legitimate of the person in charge or of a third party;

e) the recipients or the categories of recipients of the personal data, in their

case;

f) where appropriate, the intention of the controller to transfer personal data to a third party

country or international organization and the existence or absence of a decision to

adequacy of the Commission, or, in the case of transfers indicated in the

Articles 46 or 47 or Article 49, paragraph 1, second paragraph, reference to the

adequate or appropriate warranties and the means to obtain a copy of these or

to the fact that they have been borrowed.

2. In addition to the information mentioned in section 1, the person responsible for the

treatment will facilitate the interested party, at the moment in which the data is obtained

personal, the following information necessary to guarantee data processing

fair and transparent

a) the period during which the personal data will be kept or, when it is not

possible, the criteria used to determine this period;

b) the existence of the right to request from the data controller access to the

personal data relating to the interested party, and its rectification or deletion, or the limitation

of its treatment, or to oppose the treatment, as well as the right to portability

of the data;

c) when the treatment is based on article 6, paragraph 1, letter a), or article

9, paragraph 2, letter a), the existence of the right to withdraw consent in

any time, without affecting the legality of the treatment based on the

consent prior to its withdrawal;

d) the right to file a claim with a supervisory authority;

e) if the communication of personal data is a legal or contractual requirement, or a

necessary requirement to sign a contract, and if the interested party is obliged to provide

personal data and is informed of the possible consequences of not

provide such data;

f) the existence of automated decisions, including profiling, to which

referred to in article 22, sections 1 and 4, and, at least in such cases, information

about applied logic, as well as the importance and consequences

provisions of said treatment for the interested party.

3. When the data controller plans further data processing

personal data for a purpose other than that for which they were collected, you will provide the

interested party, prior to such further processing, information on that other purpose

and any additional information relevant under paragraph 2.

4. The provisions of sections 1, 2 and 3 shall not apply when and in the

to the extent that the interested party already has the information.

IV

In the present case, after studying the arguments presented, it is considered that

the conduct of the claimed party does not violate article 5 of the RGPD, which regulates the principles related to the treatment, materialized in that the personal data that are required to put the application into operation, after proving that it is not necessary for the installation of the application access to personal data stored by users on the device.

In relation to article 13 of the RGPD, it has been verified that the respondent informs duly to the complainant about the accesses, which are well informed about

the conditions of use of the application, explaining the need for access and its purpose.

v

Therefore, after learning of these facts, the Director of the Agency Spanish Data Protection RESOLVES:

FIRST: PROCEED TO FILE these proceedings.

SECOND: NOTIFY this resolution to the claimant and claimed.

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 as prescribed by the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure Common to Public Administrations, and in accordance with the provisions of the art. 112 and 123 of the aforementioned Law 39/2015, of October 1, interested parties may file, optionally, an appeal for reconsideration before the Director of the Agency

Spanish Data Protection Authority within a month from the day

following the notification of this resolution or directly contentious appeal

before the Contentious-Administrative Chamber of the National High Court,

in accordance with the provisions of article 25 and paragraph 5 of the provision

additional fourth of Law 29/1998, of July 13, regulating the Jurisdiction

Contentious-Administrative, within two months from the day after

to the notification of this act, as provided in article 46.1 of the aforementioned Law.

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es