 File No.: PS/00556/2021

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 complaining party) dated October 21, 2020 filed a claim with the Spanish Data Protection Agency.

The claim is directed against WIZINK BANK, S.A. with NIF A81831067 (in hereafter, the party claimed).

The reason on which you base your claim is the processing of your personal data by part of the claimed entity for contracting a credit card, without its consent.

The claimant, when requesting financing, finds out that it is included in files of capital solvency by HOIST FINANCE.

The complaining party requests information and is sent a copy of the contract, verifying that except for your name, surnames and ID, the other data is false (address, profession, children, income, mail, telephone, bank account...).

Attached to your written claim, among other documents, is a complaint filed with the General Directorate of the Police for possible fraud and identity theft with date of October 16, 2020.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5 December, of Protection of Personal Data and guarantee of digital rights (in hereinafter LOPDGDD), said claim was transferred to the claimed party, to to proceed with its analysis and inform this Agency within a month of the actions carried out to adapt to the requirements set forth in the regulations of

Data Protection.

On December 16, 2020, this Agency received a written response from

the respondent entity stating that it has no contractual relationship with the

claimed and therefore is not responsible for the processing of the personal data of the

claimant, basing his assertion on the assignment of the claimant's debt to the

HOIST FINANCE entity, a fact that the claimant communicated in writing to the interested party.

Such facts are confirmed by means of a copy of the communication sent to the

claimant in which they are informed of the origin of the debt, its assignment in

December 2018 to the entity HOIST FINANCE.

THIRD: On January 4, 2021, the Director of the Spanish Agency for

Data Protection agreed to admit for processing the claim presented by the party

claimant.

FOURTH: The General Subdirectorate for Data Inspection proceeded to carry out

of previous investigative actions to clarify the facts in

matter, by virtue of the investigative powers granted to the authorities of

control in article 58.1 of Regulation (EU) 2016/679 (General Regulation of

Data Protection, hereinafter RGPD), and in accordance with the provisions of the

Title VII, Chapter I, Second Section, of the LOPDGDD, having knowledge of the

following ends:

Information requested from WIZINK on the identity accreditation procedure

in the contracting of credit cards, dated June 10, 2021

receives in this Agency, written of allegations informing that for the contracting

of the credit card in question, the applicant chose the online procedure

following the procedure below:

Form completion by entering:

name and surnames, ID, age and telephone.

-

- And to continue with the process, the applicant chose “COMPLETE THE

DATA AND CONTRACT WITHOUT A CALL”

In the next step, the following data was required:

- Personal and contact information: date of birth, nationality, telephone numbers

contact information, postal address, email address, type of housing and

tenancy regime, marital status and number of children.

- Bank details: account holder and IBAN.

In the next step, the following data was required:

- Data on employment: Employment situation.

- Economic data: Non-recurring annual income.

- Professional data: Company data.

The application is held pending its final approval, proceeding to

signing and submitting the necessary documents for the contract.

To send the documentation, the applicant received an email with a link, to

through which the applicant accessed a website where he was guided through 5 simple

steps, detailed below, to complete the signature procedure

advanced electronics and attach the required documents (DNI and payroll).

The applicant sent a copy of the DNI on both sides and a copy of his last payslip.

For the advanced signature process, category of signature used according to

manifestations of WIZINK, used a trusted third party (LLEIDANETWORKS

SERVEIS TELEMATICS, S.A.) that sent an SMS with a code to the mobile number

provided by the applicant himself that he had to enter in the last step of the

contracting process on the WIZINK website. Attach certified SMS by ***URL.1

and certificate of ***URL.1 of validity of the signature

After this process, WIZINK carried out a detailed analysis of the

request concluding that said request should be approved.

This analysis was practically based on the examination of the photocopy of the DNI.

As the respondent states, "WIZINK is a digital bank that markets its

products through remote means of communication, and which has placed special

emphasis on adopting the necessary measures to comply at all times with the

obligations imposed by the regulations that apply to it when identifying

to his clients. They add that the customer identification process is the result of

the application of the regulations on the Law for the Prevention of Money Laundering and

the Financing of Terrorism, Law 10/2010 of April 28 (hereinafter, LPBC)".

For this identification, perform the following actions:

1 Link the applicant uniquely:

WIZINK identified the Applicant through a trusted third party, ***URL.1, to

through the advanced electronic signature, which made it possible to comply with the obligation to

due diligence imposed by the regulations of the LPBC. In addition, they cite article 12

of the LPBC, and its Development Regulations, in its article 21, where the

electronic signature as one of the valid and recognized requirements to use in the

contracting process through telephone, electronic or telematic means.

They maintain that this interaction with ***URL.1 allowed the applicant to become

uniquely identified at the start of the process and as it progressed through the

recruitment flow.

2 Identify the applicant, based on the collection of a series of evidence, as

Email address

3 Facilitate that the signature was made by means that the signatory could keep under his control.

exclusive control, your mobile phone.

FIFTH: On December 22, 2021, the Director of the Spanish Agency for

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

in accordance with the provisions of articles 63 and 64 of Law 39/2015, of October 1,

of the Common Administrative Procedure of the Public Administrations (in

hereinafter, LPACAP), for the alleged violation of article 6 of the RGPD and article 32 of the

RGPD, typified in Article 83.5 of the RGPD.

SIXTH: Notification of the aforementioned start-up agreement, at the request of the entity

claimed is given access to the complete file, as well as an extension of the term

to present claims.

SEVENTH: The respondent filed a pleadings brief in which, in summary,

stated that by dating the request for the card from September 2017 and being the date

notice of the December 2021 initiation agreement, such facts are found

prescribed.

It also states that in relation to the requirements related to non-compliance with

money laundering, the respondent alleges that the Spanish Agency for the Protection of

Data is not competent to observe the violations that in relation to said

matter could be committed, since these functions are assigned to the

Commission for the Prevention of Money Laundering and Monetary Offences,

dependent on the Secretary of State for the Economy.

He points out that it is not possible to determine that, both under full observance of the

regulations applicable at the time of the card request date, as well as the

regulations in force and applicable at the time of notification of this Agreement,

has incurred in a breach in relation to the security measures

applied and this is derived from the inexistence of a legal precept that obliges the

identification, since it considers that the RGPD does not apply to it, but the LOPD

15/1999.

EIGHTH: On March 9, 2022, a resolution proposal is submitted

proposing that the Director of the Spanish Data Protection Agency sanction

to WIZINK BANK, S.A. with NIF A81831067, by:

□

□

an infringement of article 6 of the RGPD typified in article 83.5.a) of the

RGPD and for prescription purposes, by article 72.1 b) of the LOPDGDD with

a fine of €100,000 (one hundred thousand euros).

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

RGPD and for prescription purposes, by article 73 g) of the LOPDGDD with

a fine of €50,000 (fifty thousand euros).

NINTH: On March 23, 2022, the respondent presents arguments to

the resolution proposal reiterating those already presented after the initial agreement

relating to the fact that the facts that are the subject of this sanctioning procedure

are prescribed, when dating the application for the card from September 2017 and being the

December 2021 start agreement notification date.

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited:

PROVEN FACTS

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/8

FIRST: A processing of personal data of the claimant by the

of the claimed entity, without its consent.

The claimant, when requesting financing, finds out that it is included in files of

capital solvency by HOIST FINANCE.

Through two claims made through the OMIC, he is aware that

the debt was purchased from WIZINK BANK, an entity with which it had allegedly

signed a credit card agreement.

They send you a copy of the contract and except your name and surnames and DNI, the rest

are false (address, profession, children, income, mail, telephone, bank account...), for

which files a complaint with the police dated October 16, 2020.

SECOND: The entity complained against alleges that the facts that are the subject of this claim

are prescribed because the card application dates from September 2017, and the

lack of competence of this Agency, as control authority.

FOUNDATIONS OF LAW

Yo

In accordance with the powers that article 58.2 of Regulation (EU) 2016/679

(General Data Protection Regulation, hereinafter RGPD), grants each

control authority and as established in articles 47 and 48.1 of the Law

Organic 3/2018, of December 5, on the Protection of Personal Data and guarantee of

digital rights (hereinafter, LOPDGDD), is competent to initiate and resolve

this procedure the Director of the Spanish Data Protection Agency.

Likewise, article 63.2 of the LOPDGDD determines that: “The procedures

processed by the Spanish Agency for Data Protection will be governed by the provisions

in Regulation (EU) 2016/679, in this organic law, by the provisions

regulations issued in its development and, as long as they do not contradict them, with a

subsidiary, by the general rules on administrative procedures.”

Article 6 of the GDPR establishes the following:

II

"1. The processing will only be lawful if at least one of the following conditions is met:

nes:

a) the interested party gave their consent for the processing of their personal data

for one or more specific purposes;

b) the treatment is necessary for the execution of a contract in which the interested party

is part of or for the application at the request of the latter of pre-contractual measures;

c) the treatment is necessary for the fulfillment of a legal obligation applicable to the

data controller;

d) the treatment is necessary to protect the vital interests of the interested party or another

Physical person;

e) the treatment is necessary for the fulfillment of a mission carried out in the interest

public or in the exercise of public powers vested in the data controller;

f) the treatment is necessary for the satisfaction of legitimate interests pursued

by the data controller or by a third party, provided that said interests

interests do not prevail or the fundamental rights and freedoms of the interest

cases that require the protection of personal data, in particular when the interested

sado be a child.

The provisions of letter f) of the first paragraph shall not apply to the processing

by public authorities in the exercise of their functions."

For its part, article 32 of the RGPD establishes the following:

"1. Taking into account the state of the art, the application costs, and the nature

nature, scope, context and purposes of the treatment, as well as risks of probability

variable and seriousness for the rights and freedoms of natural persons, the responsible

The controller and the data processor will apply appropriate technical and organizational measures.

to guarantee a level of security appropriate to the risk, which, where appropriate, includes

yeah, among others:

a) pseudonymization and encryption of personal data;

b) the ability to ensure confidentiality, integrity, availability and resilience

permanent treatment systems and services;

c) the ability to restore the availability and access to the personal data of

quickly in the event of a physical or technical incident;

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

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

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

ta the risks that the treatment of data presents, in particular as a consequence

of the accidental or unlawful destruction, loss or alteration of personal data transmitted

stored, stored or otherwise processed, or unauthorized communication or access

two to said data.

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

certification body approved under article 42 may serve as an element for

demonstrate compliance with the requirements established in section 1 of this

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 person in charge or the person in charge and having

access to personal data can only process said data following instructions

of the person in charge, unless it is obliged to do so by virtue of Union Law or

member states."

III

In the present case, the claimant denounces the processing of her personal data

without your consent by the claimed entity for the hiring of a

credit card, which generated the inclusion of your personal data in files of

solvency.

In its defense, said entity indicates the procedure used for the

accreditation of identity in the hiring of credit cards indicated in the

made room.

Despite this procedure, the investigative actions carried out by this

Agency, it follows that given the existence of this claim, in which

verified that most of the data provided by the applicant does not correspond

to the holder of the DNI, that is, that the applicant is not the holder of the DIN provided,

It follows that the application of the regulations referred to was not the

correct or was not applied with sufficient demand based on what is established in the

Article 12. Epigraph 1.a) of Law 10/2010, of April 28, on prevention of banking

capital and financing of terrorism, hereinafter LPBC, (original text

published on April 29, 2010 in force at the time of contracting), which is

subject to the claim, and which refers to Regulation (EU) 910/2014 of the

European Parliament and of the Council of July 23, 2014 (hereinafter, Regulation

eIDAS).

All this leads us to consider that the consent of the

claimant in the execution of the contract, nor the adoption of security measures

which could lead to a violation of article 6 and another of article 32

both of the RGPD.

III

Article 72.1 b) of the LOPDGDD states that “according to what is established in the

article 83.5 of Regulation (EU) 2016/679, are considered very serious and will prescribe

after three years the infractions that suppose a substantial violation of the

articles mentioned therein and, in particular, the following:

b) The processing of personal data without the concurrence of any of the conditions of

legality of the treatment in article 6 of Regulation (EU) 2016/679.”

In turn, article 73.g) of the LOPDGDD, under the heading "Infringements considered

bass has:

“According to article 83.4 of Regulation (EU) 2016/679, they will be considered serious and

Infractions that suppose a substantial violation will prescribe after two years.

of the articles mentioned therein, and in particular the following:

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

technical and organizational measures that have been implemented as required

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

IV

After a detailed study of the documents contained in this procedure

sanctioning party, it is considered that since the date of entry of the claim is October

of 2020 and the date of contracting the credit card, object of the present

sanctioning procedure, of September 2017, these facts are found

prescribed in accordance with current legislation, after more than 3

years.

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