 File No.: PS/00068/2022

RESOLUTION OF TERMINATION OF THE PROCEDURE FOR PAYMENT

VOLUNTEER

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

to the following

BACKGROUND

FIRST: On July 21, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate sanction proceedings against WUNSCHURLAUB

S.L. (hereinafter, the claimed party), through the transcribed Agreement:

<<

File No.: PS/00068/2022

IMI Reference: A56ID 165225- A61VMAN 183378- Case Register 171475

AGREEMENT TO START THE SANCTION PROCEDURE

Of the actions carried out by the Spanish Data Protection Agency and in

based on the following

FACTS

FIRST: A.A.A. (hereinafter, the claimant) filed a claim with the

data protection authority Berlin (Germany). The claim is directed against

WUNSCHURLAUB S.L. with NIF B35896000 (hereinafter, WUNSCHURLAUB).

The reasons on which the claim is based are the following:

The website www.meine-auszeit-jetzt.de stores passwords in the clear. As

registered user, the complaining party received an unencrypted email having

clicked "forgot password", which contained your personal password (chosen by the

complaining party). On June 1, 2020, the complaining party contacted the person responsible

of treatment and described the problem. On June 2, he received a reply in which

they claim that the task was assigned to the IT department and the DPD was consulted.

Along with the claim, provide:

- Capture of email sent to the complaining party from the address

einfo@meine-auszeitjetzt.de, with the subject “Your password at meine-auszeit-jetzt.de”

and the following text (in German): “Dear A.A.A., your login password

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

2/12

is: [blacked out]. With your access data you can log in now at

www.meine-auszeit-jetzt.de and make your travel request. Kind regards".

SECOND: Through the "Internal Market Information System" (hereinafter

IMI), regulated by Regulation (EU) No. 1024/2012, of the European Parliament and of the

Council, of October 25, 2012 (IMI Regulation), whose objective is to promote the

cross-border administrative cooperation, mutual assistance between States

members and the exchange of information, as of January 27, 2020, had entry

in this Spanish Data Protection Agency (AEPD) the aforementioned claim. He

transfer of this claim to the AEPD is carried out in accordance with the provisions

in article 56 of Regulation (EU) 2016/679, of the European Parliament and of the

Council, of 04/27/2016, regarding the Protection of Physical Persons in what

regarding the Processing of Personal Data and the Free Circulation of these Data

(hereinafter, GDPR), taking into account its cross-border nature and that this

Agency is competent to act as main control authority, given that

WUNSCHURLAUB has its registered office and unique establishment in Spain.

According to the information incorporated into the IMI System, in accordance with the

established in article 60 of the GDPR, acts as a "control authority

data subject", in addition to the German data protection authority in Berlin, the

German authorities in Rhineland-Palatinate, Baden-Wurttemberg, Lower Saxony and

Bavaria (Private Sector). All of them under article 4.22 of the GDPR, given that

data subjects residing in these regions are likely to be

substantially affected by the treatment object of this procedure.

THIRD: On March 12, 2021, in accordance with article 64.3 of the

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

guarantee of digital rights (LOPDGDD), the claim was admitted for processing

submitted by the complaining party.

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

of previous investigative actions to clarify the facts in

matter, by virtue of the functions assigned to the control authorities in the

article 57.1 and of the powers granted in article 58.1 of the GDPR, and of

in accordance with the provisions of Title VII, Chapter I, Second Section, of the

LOPDGDD, having knowledge of the following extremes:

WUNSCHURLAUB has been requested to provide, among other information, the

user registration procedure and password security policy. In

Specifically, information has been requested on the distribution and delivery policy of the

passwords to users, both in the registration process and in the process of

password recovery when the user uses the option "Passwort

vergessen?" (Have you forgotten your password?) and information about whether by using this

option, the user is provided with the password that he had established or is assigned a

new. Likewise, information has been requested on the method of storage of

access passwords associated with users and information on whether

stored encrypted.

WUNSCHURLAUB has stated the following:

About the registration process

The user must provide the following information during registration:

- Name and surname

-

Birthdate

-

Phone

- Address

- Email

- Password of free choice (twice, without being displayed on the screen)

At the end of the registration, the user receives a customer number, generated

automatically.

The representatives of WUNSCHURLAUB indicate that when entering the system (performing

login), the user cannot see or access their data, only the name and

surname indicating that it is in use. Password when entered never appears

in clear, always with star symbols and it is not used for accessing the data, but rather

only to allow entry to the page in order to request an offer for a

specific trip, not having any relationship with the database.

Regarding the storage of data, they only indicate in a generic way that

performed with MySQL, and that the provider is certified ISO 27001:2013 and ISO

9001:2015. The question of whether it is stored encrypted is not answered.

However, about the option “Passwort vergessen?” (Have you forgotten your password?)

WUNSCHURLAUB representatives confirm that with this option the user,

indicating your personal customer number and your date of birth, you receive an email

e-mail with a clear password, the one you chose when registering.

The representatives of WUNSCHURLAUB indicate that they want to add that they have been

faced with a case of blackmail: the complaining party has sent them an email

e-mail with the offer of its services to improve security, advising that

In the case of denying it, he would be forced to take measures, that is, denounce the

company to the authority, having answered that they are not interested in their

services, and including a detailed explanation of the use of the password.

Regarding the volume of treatments carried out: the entity has declared having

37,715 users as of April 6, 2021.

No actions have been found in the information systems of this Agency

above related to WUNSCHURLAUB.

According to AXESOR, WUNSCHURLAUB is an SME established in 2006, with 7

employees and a sales volume of 3.33 million euros (according to the

last exercise presented in 2019).

FIFTH: On February 24, 2022, the Director of the AEPD adopted a

draft decision to initiate disciplinary proceedings. following the process

established in article 60 of the GDPR, was transmitted through the IMI system this

draft decision and the authorities concerned were informed that they had

four weeks from that time to raise pertinent objections and

motivated. Within the term for this purpose, the control authorities concerned shall not

presented pertinent and reasoned objections in this regard, for which reason it is considered

that all authorities agree with said draft decision and are

linked by it, in accordance with the provisions of section 6 of article 60

of the GDPR.

This draft decision was notified to WUNSCHURLAUB in accordance with the rules

established in Law 39/2015, of October 1, on Administrative Procedure

Common Public Administrations (hereinafter, LPACAP) on March 1

of 2022, as stated in the acknowledgment of receipt that is in the file.

FUNDAMENTALS OF LAW

Competition and applicable regulations

Yo

In accordance with the provisions of articles 58.2 and 60 of Regulation (EU) 2016/679

of the European Parliament and of the Council of April 27, 2016 on the protection

of natural persons with regard to the processing of personal data and the

free circulation of these data (GDPR), and as established in articles 47,

48.1, 64.2 and 68.1 and 68.2 of Organic Law 3/2018, of December 5, Protection

of Personal Data and guarantee of digital rights (hereinafter, LOPDGDD) is

competent to initiate and resolve this procedure the Director of the Agency

Spanish Data Protection.

Likewise, article 63.2 of the LOPDGDD determines that: "Procedures

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

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

regulations dictated in its development and, insofar as they do not contradict them, with character

subsidiary, by the general rules on administrative procedures."

II

previous questions

In the present case, in accordance with the provisions of article 4.1 of the GDPR, there is

the processing of personal data, since WUNSCHURLAUB

carries out the collection and conservation of, among others, the following personal data of

natural persons: name and surname, date of birth and email, among

other treatments.

WUNSCHURLAUB carries out this activity in its capacity as person in charge of the

treatment, since it is who determines the purposes and means of such activity, by virtue of

of article 4.7 of the GDPR. In addition, it is a cross-border processing, given

that WUNSCHURLAUB is established in Spain, although it provides services to other

European Union countries.

The GDPR provides, in its article 56.1, for cases of cross-border processing,

provided for in its article 4.23), in relation to the competence of the authority of

main control, that, without prejudice to the provisions of article 55, the authority of

control of the main establishment or of the only establishment of the person in charge or of the

The person in charge of the treatment will be competent to act as control authority

for the cross-border processing carried out by said controller or

commissioned in accordance with the procedure established in article 60. In the case

examined, as has been exposed, WUNSCHURLAUB has its unique establishment

in Spain, so the Spanish Agency for Data Protection is competent

to act as the main supervisory authority.

For its part, article 4 section 12 of the GDPR defines, in a broad way, the

“personal data security violations” (hereinafter security breach)

as "all those violations of security that cause the destruction,

accidental or unlawful loss or alteration of personal data transmitted, stored

or otherwise processed, or unauthorized disclosure of or access to such data.”

In the present case, there is a personal data security breach in the

circumstances indicated above, categorized as a breach of confidentiality, by

passwords of the users of the website meine-auszeit-jetzt.de are sent to each other at

clear.

It should be noted that the identification of a security breach does not imply the

imposition of a sanction directly by this Agency, since it is necessary

analyze the diligence of managers and managers and security measures

applied.

Within the principles of treatment provided for in article 5 of the GDPR, the

integrity and confidentiality of personal data is guaranteed in section 1.f)

of article 5 of the GDPR. For its part, the security of personal data comes

regulated in article 32 of the GDPR, which regulates the security of the treatment.

II

Security measures

Article 32 "Security of treatment" of the GDPR establishes:

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

nature, scope, context and purposes of processing, 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 and

appropriate organizational measures to guarantee a level of security appropriate to the risk,

which may include, among others:

a) the 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 assessment of effectiveness

technical and organizational measures to guarantee the safety of the

treatment.

2. When evaluating the adequacy of the security level, particular consideration will be given to

take into account the risks presented by data processing, in particular as

consequence of the destruction, loss or accidental or illegal alteration of data

personal information transmitted, preserved or processed in another way, or the communication or

unauthorized access to such data.

3. Adherence to an approved code of conduct pursuant to 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 controller and the processor shall take measures to ensure that

any person acting under the authority of the controller or processor and

have access to personal data can only process such data by following

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.

In the present case, at the time the breach occurred, it is clear that

WUNSCHURLAUB sent all users who made use of its website

the option “Passwort vergessen?” (Have you forgotten your password?) an email

with a clear password, the one that the user had chosen when registering,

with which it is verified that it was possible to access the user's password to

send it to him in case of forgetfulness and that the security measures are, by all accounts,

insufficient.

According to the evidence available at this time in

agreement to start disciplinary proceedings, and without prejudice to what results from the

investigation, it is considered that the known facts could constitute a

infringement, attributable to WUNSCHURLAUB, for violation of article 32 of the GDPR.

Classification of the infringement of article 32 of the GDPR

IV.

If confirmed, the aforementioned infringement of article 32 of the GDPR could lead to the

commission of the offenses typified in article 83.4 of the GDPR that under the

The heading "General conditions for the imposition of administrative fines" provides:

Violations of the following provisions will be sanctioned, in accordance with the

paragraph 2, with administrative fines of maximum EUR 10,000,000 or,

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

total annual global business volume of the previous financial year, opting for

the highest amount:

a) the obligations of the person in charge and the person in charge according to articles 8,

11, 25 to 39, 42 and 43; (…)”

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that

"The acts and behaviors referred to in sections 4,

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

contrary to this organic law”.

For the purposes of the limitation period, article 73 "Infractions considered serious"

of the LOPDGDD indicates:

"Based on what is established in 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:

(…)

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”. (…)

Penalty for violation of article 32 of the GDPR

V

For the purposes of deciding on the imposition of an administrative fine and its amount,

In accordance with the evidence available at the present time of

agreement to start disciplinary proceedings, and without prejudice to what results from the

instruction, it is considered appropriate to graduate the sanction to be imposed in accordance with

the following criteria established in article 83.2 of the GDPR:

As aggravating factors:

-

The nature, seriousness and duration of the infringement, taking into account the

nature, scope or purpose of the processing operation in question

such as the number of interested parties affected and the level of damages that

have suffered (section a): due to the storage of passwords without the measures

adequate security, of at least 37,715 users, from June 1,

2020 to present.

The balance of the circumstances contemplated in article 83.2 of the GDPR, with

regarding the infringement committed by violating the provisions of article 32 of the GDPR,

initially allows a penalty of €3,000 (three thousand euros) to be set.

SAW

imposition of measures

If the infringement is confirmed, it could be agreed to impose on the person responsible that within the term

within 60 days, proceed to adapt the storage of your users' passwords

so that they are not stored in the clear and to implement a new procedure so that

Users can recover their passwords, according to what has already been indicated, without

detriment of others that may derive from the instruction of the procedure, from

In accordance with the provisions of the aforementioned article 58.2 d) of the GDPR, according to which each

The supervisory authority may “order the person in charge or in charge of the treatment to

processing operations comply with the provisions of this

Regulation, where appropriate, in a certain way and within a time limit

specified…". The imposition of this measure is compatible with the sanction

consisting of an administrative fine, according to the provisions of art. 83.2 of the GDPR.

Likewise, the measures that could be adopted in the resolution that puts an end to the

procedure, in relation to the storage of passwords, would be of

application in all countries of the European Union in which it operates

WUNSCHURLAUB.

It is noted that not meeting the requirements of this body could be

considered as an administrative offense in accordance with the provisions of the GDPR,

classified as an infraction in its article 83.5 and 83.6, being able to motivate such conduct the

opening of a subsequent administrative sanctioning procedure.

Therefore, in accordance with the foregoing, by the Director of the Agency

Spanish Data Protection,

HE REMEMBERS:

FIRST: INITIATE SANCTION PROCEDURE against WUNSCHURLAUB S.L.,

with NIF B35896000, for the alleged violation of Article 32 of the GDPR, typified in

Article 83.4 of the GDPR.

SECOND: APPOINT as instructor R.R.R. and, as secretary, S.S.S., indicating

that any of them may be challenged, where appropriate, in accordance with the provisions of

Articles 23 and 24 of Law 40/2015, of October 1, on the Legal Regime of the

Public Sector (LRJSP).

THIRD: INCORPORATE into the disciplinary file, for evidentiary purposes, the

documentation from IMI that has given rise to the previous actions of

investigation, as well as the documents obtained and generated by the Subdirectorate

General of Data Inspection in the actions prior to the start of this

disciplinary procedure and documentation from IMI on the project

decision.

FOURTH: THAT for the purposes provided for in art. 64.2 b) of Law 39/2015, of 1

October, of the Common Administrative Procedure of Public Administrations

sanction that could correspond would be 3000.00 euros, without prejudice to what

results from the instruction.

FIFTH: NOTIFY this agreement to WUNSCHURLAUB S.L., with NIF

B35896000, granting a hearing period of ten business days to formulate

the allegations and present the evidence it deems appropriate. In his writing of

allegations must provide your NIF and the procedure number that appears in the

heading of this document.

If, within the stipulated period, he does not make allegations to this initial agreement, the same

may be considered a resolution proposal, as established in article

64.2.f) of Law 39/2015, of October 1, on the Common Administrative Procedure of

Public Administrations (hereinafter, LPACAP).

In accordance with the provisions of article 85 of the LPACAP, you may recognize your

responsibility within the period granted for the formulation of allegations to the

present initiation agreement; which will entail a reduction of 20% of the

sanction that should be imposed in this proceeding. With the application of this

reduction, the sanction would be established at 2,400.00 euros, resolving the

procedure with the imposition of this sanction.

In the same way, it may, at any time prior to the resolution of this procedure, carry out the voluntary payment of the proposed sanction, which will mean a reduction of 20% of its amount. With the application of this reduction, the sanction would be established at 2,400.00 euros and its payment will imply the termination of the procedure.

The reduction for the voluntary payment of the penalty is cumulative to the corresponding apply for acknowledgment of responsibility, provided that this acknowledgment of the responsibility is revealed within the period granted to formulate allegations at the opening of the procedure. Voluntary payment of the referred amount in the previous paragraph may be done at any time prior to the resolution. In In this case, if both reductions were to be applied, the amount of the penalty would remain established at 1,800.00 euros.

In any case, the effectiveness of any of the two aforementioned reductions will be conditioned to the withdrawal or resignation of any action or appeal via administrative against the sanction.

In the event that you choose to proceed with the voluntary payment of any of the amounts indicated above (2,400.00 euros or 1,800.00 euros), you must make it effective by depositing it in the account number ES00 0000 0000 0000 0000 0000 opened to name of the Spanish Data Protection Agency in the bank CAIXABANK, S.A., indicating in the concept the reference number of the procedure that appears in the heading of this document and the cause of reduction of the amount to which it receives.

Likewise, you must send proof of income to the General Subdirectorate of Inspection to continue with the procedure in accordance with the quantity entered.

The procedure will have a maximum duration of nine months from the

date of the initiation agreement or, where appropriate, of the draft initiation agreement.

After this period, its expiration will occur and, consequently, the file of

performances; in accordance with the provisions of article 64 of the LOPDGDD.

Finally, it is noted that in accordance with the provisions of article 112.1 of the

LPACAP, there is no administrative appeal against this act.

935-110422

Mar Spain Marti

Director of the Spanish Data Protection Agency

>>

SECOND: On July 27, 2022, the claimed party has proceeded to pay

the penalty in the amount of 1800 euros making use of the two reductions provided

in the Commencement Agreement transcribed above, which implies recognition of the

responsibility.

THIRD: The payment made, within the period granted to formulate allegations to

the opening of the procedure, entails the waiver of any action or appeal via

against the sanction and acknowledgment of responsibility in relation to

the facts referred to in the Commencement Agreement.

FOURTH: In the previously transcribed initiation agreement, it was indicated that, if

Once the infringement is confirmed, it could be agreed to impose on the controller the adoption of

adequate measures to adjust its performance to the regulations mentioned in this

act, in accordance with the provisions of the aforementioned article 58.2 d) of the GDPR, according to the

which each control authority may "order the person responsible or in charge of the

processing that the processing operations comply with the provisions of the

this Regulation, where appropriate, in a certain way and within a certain

specified term…".

Having recognized the responsibility for the infringement, the imposition of

the measures included in the Initiation Agreement.

FUNDAMENTALS OF LAW

Yo

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

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

control authority and as established in articles 47, 48.1, 64.2 and 68.1 of the

Organic Law 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 Protection Agency

of data.

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

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

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

regulations dictated in its development and, insofar as they do not contradict them, with character

subsidiary, by the general rules on administrative procedures."

II

Article 85 of Law 39/2015, of October 1, on Administrative Procedure

Common for Public Administrations (hereinafter, LPACAP), under the heading

"Termination in disciplinary proceedings" provides the following:

"1. Initiated a disciplinary procedure, if the offender acknowledges his responsibility,

The procedure may be resolved with the imposition of the appropriate sanction.

2. When the sanction has only a pecuniary nature or it is possible to impose a

pecuniary sanction and another of a non-pecuniary nature but the

inadmissibility of the second, the voluntary payment by the presumed perpetrator, in

any moment prior to the resolution, will imply the termination of the procedure,

except in relation to the replacement of the altered situation or the determination of the

compensation for damages caused by the commission of the offence.

3. In both cases, when the sanction is solely pecuniary in nature, the

The competent body to resolve the procedure will apply reductions of at least

20% of the amount of the proposed penalty, these being cumulative among themselves.

The aforementioned reductions must be determined in the notification of initiation

of the procedure and its effectiveness will be conditioned to the withdrawal or resignation of

any administrative action or resource against the sanction.

The percentage reduction provided for in this section may be increased

according to regulations."

According to what has been stated,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: DECLARE the termination of procedure PS/00068/2022, in

in accordance with the provisions of article 85 of the LPACAP.

SECOND: REQUIRE WUNSCHURLAUB S.L. so that within a month

notify the Agency of the adoption of the measures described in the

legal foundations of the initiation agreement transcribed in this resolution.

THIRD: NOTIFY this resolution to WUNSCHURLAUB S.L..

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

Resolution will be made public once the interested parties have been notified.

Against this resolution, which puts an end to the administrative process as prescribed by

the art. 114.1.c) of Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations, interested parties may file an appeal

administrative litigation before the Administrative Litigation 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 for in article 46.1 of the

referred Law.

Mar Spain Marti

Director of the Spanish Data Protection Agency

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es