 Procedure No.: PS/00287/2020

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. (hereinafter, the claimant) on 04/22/2020 filed

claim before the Spanish Data Protection Agency. The claim is

directed against COMERCIO ONLINE LEVANTE, S.L. with NIF B12983292 (hereinafter,

the claimed). The reasons on which the claim is based are that when trying to access

your user account in perfumespremium.es will show the personal data of

a different user.

Provides screen printing showing the data of another client, with registered address

in Castelldefels, Barcelona.

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

Data Inspection proceeded to carry out the following actions:

On 06/04/2020, the claim submitted was transferred to the claimant for analysis

and communication to the claimant of the decision adopted in this regard. Likewise, it

required so that within a month it would send to the Agency determined

information:

- The decision adopted regarding this claim.

- In the event of exercising the rights regulated in articles 15 to 22

of the RGPD, accreditation of the response provided to the claimant.

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

claim.

- Report on the measures adopted to prevent the occurrence of

similar incidents, dates of implementation and controls carried out to

check its effectiveness.

- Any other that you consider relevant.

The Agency does not record a response to the transfer of the claim.

THIRD: On 09/06/2020, in accordance with article 65 of the LOPDGDD, the

Director of the Spanish Agency for Data Protection agreed to admit for processing the

claim filed by the claimant against the respondent.

FOURTH: On 10/08/2020, the Director of the Spanish Protection Agency

of Data agreed to initiate a sanctioning procedure against the defendant, for the alleged

Infractions of articles 5.1.f) and 32.1 of the RGPD, typified in article 83.5.a)

83.4.a) of the GDPR.

FIFTH: Once the initiation agreement has been notified, the one claimed at the time of this

The resolution has not presented a written statement of allegations, for which reason the

indicated in article 64 of Law 39/2015, of October 1, on the Procedure

Common Administrative Law of Public Administrations, which in section f)

establishes that in the event of not making allegations within the period established on the

content of the initiation agreement, it may be considered a proposal for

resolution when it contains a precise statement about the responsibility

imputed, reason why a Resolution is issued.

SIXTH: Of the actions carried out in this proceeding, they have been

accredited the following:

PROVEN FACTS

FIRST: On 01/21/2020 there is a written entry in the AEPD from the interested party in which declares that the website perfumespremium.es shows personal data, addresses and billing of other users when trying to log in with their own profile.

SECOND: The claimant provides a screen print of the aforementioned web page in the that the data of another client, with address in Castelldefels, Barcelona, is observed.

THIRD: The claimant provides a copy of the e-mail sent to perfumespremium.es on 04/26/2020 in which he states the following:

To: info@ perfumespremium.com

Good evening, when trying to enter my profile to check the processing of my request, puts me in the profile of other users, showing me their personal data, billing address and order history. I need to know how my order is going and its arrival date as I cannot track it.

Order number: Order # 8000042803

FOURTH: The claimed privacy policy is provided in accordance with the new RGPD, although the complainant points out that there is no way to contact the company or through the contact telephone number or email indicated in their website.

FOUNDATIONS OF LAW

By virtue of the powers that article 58.2 of the RGPD recognizes to each control authority, 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 solve this procedure.

Yo

Law 39/2015, of October 1, on the Common Administrative Procedure of

the Public Administrations, in its article 64 "Agreement of initiation in the

procedures of a sanctioning nature", provides:

II

"1. The initiation agreement will be communicated to the instructor of the procedure, with

transfer of how many actions exist in this regard, and the interested parties will be notified,

understanding in any case by such the accused.

Likewise, the initiation will be communicated to the complainant when the rules

regulators of the procedure so provide.

2. The initiation agreement must contain at least:

a) Identification of the person or persons allegedly responsible.

b) The facts that motivate the initiation of the procedure, its possible

rating and sanctions that may apply, without prejudice to what

result of the instruction.

c) Identification of the instructor and, where appropriate, Secretary of the procedure, with

express indication of the system of recusal of the same.

d) Competent body for the resolution of the procedure and regulation that

attribute such competence, indicating the possibility that the presumed

responsible can voluntarily acknowledge their responsibility, with the

effects provided for in article 85.

e) Provisional measures that have been agreed by the body

competent to initiate the sanctioning procedure, without prejudice to those that

may be adopted during the same in accordance with article 56.

f) Indication of the right to formulate allegations and to the hearing in the

procedure and the deadlines for its exercise, as well as an indication that, in

If you do not make allegations within the stipulated period on the content of the

initiation agreement, this may be considered a resolution proposal

when it contains a precise statement about the responsibility

imputed.

3. Exceptionally, when at the time of issuing the initiation agreement

there are not sufficient elements for the initial qualification of the facts that motivate

the initiation of the procedure, the aforementioned qualification may be carried out in a phase

later by drawing up a List of Charges, which must be notified to

the interested".

In application of the previous precept and taking into account that no

formulated allegations to the initial agreement, it is appropriate to resolve the initiated procedure.

III

Article 58 of the RGPD, Powers, states:

"two. Each supervisory authority will have all of the following powers

corrections listed below:

(…)

i) impose an administrative fine under article 83, in addition to or in

Instead of the measures mentioned in this section, according to the

circumstances of each particular case;

(…)"

In the first place, article 5 of the RGPD establishes the principles that must be govern the processing of personal data and mentions among them that of "integrity and confidentiality".

The cited article states that:

"1. The personal data will be:

(…)

f) treated in such a way as to ensure adequate security of the personal data, including protection against unauthorized processing or against its loss, destruction or accidental damage, through the application of appropriate technical or organizational measures ("integrity and confidentiality")".

(…)

Article 5, Duty of confidentiality, of the new Organic Law 3/2018, of 5 December, Protection of Personal Data and guarantee of digital rights (hereinafter LOPDGDD), states that:

"1. Those responsible and in charge of data processing as well as all people who intervene in any phase of this will be subject to the duty of confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary of the duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will remain even when the relationship of the obligor with the person in charge or person in charge had ended of the treatment".

IV

The documentation in the file shows that the claimed,

violated article 5 of the RGPD, principles related to the treatment, in relation to the

Article 5 of the LOPGDD, duty of confidentiality, by allowing access to the

claimant to the personal data of a third person when accessing your account

user in perfumespremium.es where the personal data of another client appears.

This duty of confidentiality, previously the duty of secrecy, must

understood that its purpose is to prevent leaks of data not

consented to by their owners.

Therefore, this duty of confidentiality is an obligation that falls not

only to the person in charge and in charge of the treatment but to everyone who intervenes in

any phase of the treatment and complementary to the duty of professional secrecy.

Article 83.5 a) of the RGPD, considers that the infringement of "the principles

basic for the treatment, including the conditions for the consent in accordance with

of articles 5, 6, 7 and 9" is punishable, in accordance with section 5 of the

v

mentioned article 83 of the aforementioned GDPR, "with administrative fines of €20,000,000

maximum or, in the case of a company, an amount equivalent to 4% as

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

opting for the highest amount.

On the other hand, the LOPDGDD, for prescription purposes, in its article 72 indicates:

"Infringements considered very serious:

1. Based on the provisions of article 83.5 of the Regulation (EU)

2016/679 are considered very serious and the infractions that

suppose a substantial violation of the articles mentioned in that and, in

particularly the following:

a) The processing of personal data violating the principles and guarantees

established in article 5 of Regulation (EU) 2016/679.

(…)"

Second, it should be noted that the security of personal data

It is regulated in articles 32, 33 and 34 of the RGPD.

SAW

Article 32 of the RGPD "Security of treatment", establishes 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

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".

The violation of article 32 of the RGPD is typified in the article

83.4.a) of the aforementioned RGPD in the following terms:

"4. Violations of the following provisions will be sanctioned, in accordance

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

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

global total annual turnover of the previous financial year, opting for

the largest amount:

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

11, 25 to 39, 42 and 43.

(…)”

For its part, the LOPDGDD in its article 71, Violations, states 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.

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:

(…)

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

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

to what is required by article 32.1 of Regulation (EU) 2016/679”.

(…)”

The facts revealed in this claim materialize

in the access to the personal data of a third person user client of the

claimed when accessing your account at perfumespremium.es in violation of the measures

technical and organizational.

The GDPR defines personal data security breaches as

“all those violations of security that cause the destruction, loss or

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

otherwise, or unauthorized communication or access to such data”.

7th

From the documentation in the file, it is proven that the respondent has violated article 32 of the RGPD, when a security incident occurred in your system allowing access to personal data of third parties, when accessing your account the claimant in perfumespremium.es, where the data of another client with breach of security measures.

It should be noted that the RGPD in the aforementioned provision does not establish a list of the security measures that are applicable according to the data that is object of treatment, but it establishes that the person in charge and the person in charge of the treatment will apply technical and organizational measures that are appropriate to the risk that the treatment entails, taking into account the state of the art, the costs of application, the nature, scope, context and purposes of the treatment, the risks of probability and seriousness for the rights and freedoms of the persons concerned.

Likewise, the security measures must be adequate and proportionate to the detected risk, pointing out that the determination of the measures technical and organizational information must be carried out taking into account: pseudonymization and encryption, the ability to ensure the confidentiality, integrity, availability and resiliency, the ability to restore availability and access to data after a incident, verification process (not audit), evaluation and assessment of the effectiveness of the measures.

In any case, when evaluating the adequacy of the level of security, particularly taking into account the risks presented by the processing of data, such 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 and that could cause damages

physical, material or immaterial.

In this same sense, recital 83 of the RGPD states that:

"(83) In order to maintain security and prevent the treatment from violating the

provided in this Regulation, the person in charge or the person in charge must evaluate

the risks inherent to the treatment and apply measures to mitigate them, such as

encryption. These measures must guarantee an adequate level of security, including

confidentiality, taking into account the state of the art and the cost of its application

regarding the risks and the nature of the personal data that must be

protect yourself. When assessing the risk in relation to data security,

take into account the risks arising from the processing of personal data,

such as the accidental or unlawful destruction, loss or alteration of personal data

transmitted, stored or otherwise processed, or the communication or access is not

authorized to said data, susceptible in particular to cause damages

physical, material or immaterial.

In the present case, as evidenced by the facts and within the framework of the

investigation file E/03847/2020, the AEPD transferred the defendant on

06/04/2020, the claim submitted for analysis requesting the contribution of

information related to the claimed incidence, without it having been received in this

body any response.

The responsibility of the claimed party is determined by the incidence of
security revealed by the claimant, since it is responsible for taking
decisions aimed at effectively implementing technical measures and
appropriate organizational measures to guarantee a level of security appropriate to the risk
to ensure the confidentiality of the data, restoring its availability and preventing
access to them in the event of a physical or technical incident. However, from the
The documentation provided shows that the entity has not only breached this
obligation, but also the adoption of measures in this regard is unknown, despite
of having notified him of the claim filed.

In accordance with the foregoing, it is estimated that the respondent would be
also allegedly responsible for the violation of the RGPD: the violation of the
article 32, offense typified in article 83.4.a).

In order to establish the administrative fine to be imposed,
observe the provisions contained in articles 83.1 and 83.2 of the RGPD, which
point out:

viii

"1. Each control authority will guarantee that the imposition of fines
administrative actions under this article for violations of this
Regulation indicated in sections 4, 5 and 6 are in each individual case
effective, proportionate and dissuasive.

2. Administrative fines will be imposed, depending on the circumstances
of each individual case, in addition to or as a substitute for the measures contemplated
in article 58, paragraph 2, letters a) to h) and j). When deciding to impose a fine
administration and its amount in each individual case will be duly taken into account:

a) the nature, seriousness and duration of the offence, taking into account the

nature, scope or purpose of the processing operation in question

as well as the number of stakeholders affected and the level of damage and

damages they have suffered;

b) intentionality or negligence in the infringement;

c) any measure taken by the controller or processor

to alleviate the damages suffered by the interested parties;

d) the degree of responsibility of the person in charge or of the person in charge of the

treatment, taking into account the technical or organizational measures that have

applied under articles 25 and 32;

e) any previous infraction committed by the person in charge or the person in charge of the

treatment;

f) the degree of cooperation with the supervisory authority in order to put

remedying the breach and mitigating the possible adverse effects of the breach;

g) the categories of personal data affected by the infringement;

h) the way in which the supervisory authority became aware of the infringement, in

particular if the person in charge or the person in charge notified the infringement and, in such case,

what extent;

i) when the measures indicated in article 58, paragraph 2, have been

previously ordered against the person in charge or the person in charge in question

in relation to the same matter, compliance with said measures;

j) adherence to codes of conduct under article 40 or mechanisms

certificates approved in accordance with article 42, and

k) any other aggravating or mitigating factor applicable to the circumstances of the

case, such as financial benefits realized or losses avoided, direct

or indirectly, through infringement.

In relation to letter k) of article 83.2 of the RGPD, the LOPDGDD, in its article 76,

“Sanctions and corrective measures”, establishes that:

"two. 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 treatments

of personal data.

c) The profits obtained as a result of committing the offence.

d) The possibility that the conduct of the affected party could have induced the

commission of the offence.

e) The existence of a merger by absorption process after 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 those and any

interested."

data.

In accordance with the precepts transcribed, in order to set the amount of the

sanction to be imposed in the present case for the infraction typified in article 83.5.a)

of the RGPD for which the claimed party is responsible, the

following factors:

The scope in a local environment of the treatment carried out by the entity

claimed.

The number of people affected is unknown, although the claim only comes from

only one person.

The measures adopted by the respondent to prevent him from being

produce similar incidents, since before the informative requirement of the

Agency has not responded to it, which in turn affects the absence of

cooperation with the supervisory authority in order to remedy the infringement and

mitigate its possible adverse effects.

There is no evidence that the entity had acted maliciously, although

the performance reveals a serious lack of diligence.

The link between the activity of the offender and the performance of treatment of

Personal data.

The claimed entity is a small business.

- Secondly, in order to set the amount of the sanction to be imposed in the

this case for the infringement typified in article 83.4.a) of the RGPD, it is estimated

concurrent the following factors:

The scope in a local environment of the treatment carried out by the entity

claimed.

The number of people affected is unknown, although the claim only comes from

only one person.

The measures adopted by the respondent to prevent him from being

produce similar incidents, since before the informative requirement of the

Agency has not responded to it, which in turn affects the absence of

cooperation with the supervisory authority in order to remedy the infringement and

mitigate its possible adverse effects.

There is no evidence that the entity had acted maliciously, although

the performance reveals a serious lack of diligence.

The link between the activity of the offender and the performance of treatment of

Personal data.

The claimed entity is a small business.

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 COMERCIO ONLINE LEVANTE, S.L., with NIF B12983292,

for an infringement of article 5.1.f) of the RGPD, typified in article 83.5.a) of the

GDPR, a penalty of €1,000 (one thousand euros).

SECOND: IMPOSE COMERCIO ONLINE LEVANTE, S.L., with NIF B12983292,

for an infringement of article 32.1 of the RGPD, typified in article 83.4.a) of the

RGPD, a penalty of €2,000 (two thousand euros).

THIRD: NOTIFY this resolution to COMERCIO ONLINE LEVANTE, S.L.

FOURTH: 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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

11/11

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

Spanish Department of Data Protection in the banking entity CAIXABANK, S.A.. In case

Otherwise, it will be collected in the executive period.

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

between the 1st and 15th of each month, both inclusive, the term to make the payment

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

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

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

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 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 month from

counting 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,

may provisionally suspend the firm resolution in administrative proceedings if the

The interested party expresses his intention to file a contentious-administrative appeal.

If this is the case, the interested party must formally communicate this fact by

writing addressed to the Spanish Agency for Data Protection, presenting it through

Electronic Register of the Agency [https://sedeagpd.gob.es/sede-electronica-

web/], or through any of the other registers provided for in art. 16.4 of the

aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the

documentation proving the effective filing of the contentious appeal-

administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative within a period of two months from the day following the

notification of this resolution 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