

□ File No.: EXP202104873

RESOLUTION OF SANCTIONING 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 claiming party) dated November 2,
2021 filed a claim with the Spanish Data Protection Agency. The
claim is directed against INDECEMI, S.L. with NIF B98845936 (INDECEMI). The

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

He started a claim process with INDECEMI and received an email with the details of
another person who was also in the claim process, who, in turn, received
an email with the data of the complaining party.

Along with the notification, the claim sheet submitted to INDECEMI is provided, and
an email received where they apologize for the mistake made.

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

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of
October 1, of the Common Administrative Procedure of the Administrations
Public (hereinafter, LPACAP) by electronic notification, was not collected by
the person in charge, within the period of availability, understood as rejected
in accordance with the provisions of art. 43.2 of the LPACAP dated 12/18/2021, as stated

in the certificate in the file.

Although the notification was validly made by electronic means, assuming that carried out the procedure in accordance with the provisions of article 41.5 of the LPACAP, under information, a copy was sent by postal mail, which was duly notified in date 01/10/2022. In said notification, he was reminded of his obligation to relate electronically with the Administration, and they were informed of the means of access to said notifications, reiterating that, henceforth, he would be notified exclusively by electronic means.

No response has been received to this letter of transfer.

THIRD: On February 2, 2022, in accordance with article 65 of the LOPDGDD, the claim presented by the claimant party was admitted for processing.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

2/8

FOURTH: On August 22, 2022, the Director of the Spanish Agency for Data Protection agreed to initiate disciplinary proceedings against the claimed party, for the alleged violation of Article 5.1.f) of the GDPR and Article 32 of the GDPR, typified in Article 83.5 of the GDPR.

FIFTH: Notified of the aforementioned start-up agreement in accordance with the rules established in Law 39/2015, of October 1, on the Common Administrative Procedure of Public Administrations (hereinafter, LPACAP), on 08/31/2022, and after the term granted for the formulation of allegations, it has been verified that there has been no received any allegation by the claimed party.

Article 64.2.f) of the LPACAP -provision of which the claimed party was informed

in the agreement to open the procedure - establishes that if no arguments within the established term on the content of the initiation agreement, when it contains a precise pronouncement about the imputed responsibility, may be considered a resolution proposal. In the present case, the agreement of beginning of the disciplinary file determined the facts in which the imputation, the infringement of the GDPR attributed to the defendant and the sanction that could impose. Therefore, taking into consideration that the claimed party has not made allegations to the agreement to start the file and in attention to what established in article 64.2.f) of the LPACAP, the aforementioned initiation agreement is considered in the present case resolution proposal.

In view of all the proceedings, by the Spanish Agency for Data Protection

In this proceeding, the following are considered proven facts:

PROVEN FACTS

FIRST AND ONLY: It is proven that the complaining party initiated a process of claim with INDECEMI and received an email with personal data (name, surname, NIF, address, telephone and email address) of another person who was also in the claim process, who, in turn, received an email email with the personal data of the claimant.

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 and 48.1 of the Law Organic 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 Spanish Data Protection Agency.

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."

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

3/8

II

In the present case, in accordance with the provisions of article 4.1 of the GDPR, there is the processing of personal data, since INDECEMI carries out, among other treatments, the collection, registration, use, etc. of the following data personal information of natural persons, such as: name, identification number, number phone number, email address etc.

INDECEMI carries out this activity in its capacity as data controller, given who is the one who determines the purposes and means of such activity, by virtue of article 4.7 of the GDPR.

Article 4 paragraph 12 of the GDPR defines, in a broad way, "violations of security of personal data" (hereinafter security breach) as "all those security violations that cause the destruction, loss or alteration accidental or unlawful personal data transmitted, stored or otherwise processed form, or unauthorized communication or access to said data."

In the present case, there is a personal data security breach in the circumstances indicated above, categorized as a breach of confidentiality, by

been sent by email to another INDECEMI client, the data sheet

claim of the claiming party, in which their personal data is recorded.

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 to 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 articles 32, 33 and 34 of the GDPR, which regulate the security of the treatment, the notification of a breach of the security of personal data to the control authority, as well as the communication to the interested party, respectively.

Article 5.1.f) "Principles relating to processing" of the GDPR establishes:

II

"1. Personal data will be:

(...)

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

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

In the present case, it is clear that the personal data of the complaining party, obtained in the INDECEMI database, were improperly exposed to a third party, to the send to one person the claim form submitted by another.

Article 83.5 of the GDPR under the heading "General conditions for the imposition of administrative fines" provides:

IV.

Violations of the following provisions will be sanctioned, in accordance with the paragraph 2, with administrative fines of maximum EUR 20,000,000 or, in the case of a company, an amount equivalent to a maximum of 4% of the total annual global business volume of the previous financial year, opting for the highest amount:

a) the basic principles for the treatment, including the conditions for the consent under articles 5, 6, 7 and 9; (...)"

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 72 "Infractions considered very serious" of the LOPDGDD indicates:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679, are considered very serious and will prescribe after three years the infractions that a substantial violation of the articles mentioned therein and, in particular, the following:

a) The processing of personal data in violation of the principles and guarantees established in article 5 of Regulation (EU) 2016/679. (...)"

Penalty for violation of article 5.1.f) of the GDPR

V

For the purposes of deciding on the imposition of an administrative fine and its amount considers that the infringement in question is serious for the purposes of the GDPR, and that it is appropriate to graduate the sanction to be imposed according to the following criteria that Article 83.2 of the GDPR establishes:

As mitigations:

- The nature, seriousness and duration of the infringement, 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 (section a). In the present case, only

Two people were affected, and there is no record that they were caused some serious harm.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

5/8

Likewise, it is considered appropriate to graduate the sanction to be imposed in accordance with the following criteria established in section 2 of article 76 "Sanctions and measures corrective measures" of the LOPDGDD:

As mitigations:

- The linking of the offender's activity with the performance of processing of personal data (section b): The commercial activity of INDECMI, wholesale office furniture, does not indicate that handle a large amount of personal data

The balance of the circumstances contemplated in article 83.2 of the GDPR and the

Article 76.2 of the LOPDGDD, with respect to the offense committed by violating the established in article 5.1.f) of the GDPR, allows setting a penalty of €3,000 (three thousand euros).

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

SAW

"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 guarantee the confidentiality, integrity, availability and permanent resilience of treatment systems and services;
- c) the ability to restore the availability and access to personal 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.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

6/8

In the present case, at the time the breach occurred, it cannot be said that INDECEMI had the appropriate measures to avoid the incident, since it sent a claim form with personal data to a different client.

Article 83.4 of the GDPR under the heading "General conditions for the imposition of administrative fines" provides:

VII

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 ensure a level of security appropriate to the risk of treatment, in the terms required by article 32.1 of the Regulation (EU) 2016/679. (...)

VIII

For the purposes of deciding on the imposition of an administrative fine and its amount considers that the infringement in question is serious for the purposes of the GDPR, and that it is appropriate to graduate the sanction to be imposed in accordance with the criteria established by the article 83.2 of the GDPR and section 2 of article 76 "Sanctions and measures corrective measures" of the LOPDGDD:

The balance of the circumstances contemplated in article 83.2 of the GDPR and the Article 76.2 of the LOPDGDD, with respect to the offense committed by violating the established in article 32 of the GDPR, allows a penalty of €2,000 (two thousand euro).

Therefore, in accordance with the applicable legislation and assessed the criteria of graduation of sanctions whose existence has been accredited, the Director of the Spanish Data Protection Agency RESOLVES:

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/8

FIRST: IMPOSE INDECEMI, S.L., with NIF B98845936, for a violation of the Article 5.1.f) of the GDPR, typified in Article 83.5 of the GDPR, a fine of €3,000 (THREE THOUSAND EUROS)

IMONER to INDECEMI S.L. with NIF B98845936, for a violation of Article 32 of the GDPR, typified in article 83.4 of the GDPR, a fine of €2,000 (TWO THOUSAND EURO)

SECOND: NOTIFY this resolution to INDECEMI, S.L.

THIRD: Warn the penalized person that they must make the imposed sanction effective

Once this resolution is enforceable, in accordance with the provisions of Article art. 98.1.b) of Law 39/2015, of October 1, on Administrative Procedure

Common of Public Administrations (hereinafter LPACAP), within the payment period

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, by means of its income, indicating the NIF of the sanctioned and the number

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

restricted number ES00 0000 0000 0000 0000 0000, open in the name of the Agency

Spanish Data Protection Agency at the bank CAIXABANK, S.A.. In the event

Otherwise, it will proceed to its collection in the executive period.

Once the notification has been received and once executed, if the execution date 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 or immediately following business month, and if

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

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

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 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 reversal before the

Director of the Spanish Agency for Data Protection within a period of one month from

count 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 for in article 46.1 of the

referred Law.

Finally, it is noted 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 through

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

of the Electronic Registry of the Agency [[https://sedeagpd.gob.es/sede-electronica-](https://sedeagpd.gob.es/sede-electronica-web/)

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

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

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

8/8

documentation proving the effective filing of the contentious appeal-

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

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

Notification of this resolution would terminate the precautionary suspension.

Mar Spain Marti

Director of the Spanish Data Protection Agency

938-120722

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es