 File No.: PS/00020/2022

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 CLAIMING PARTY) dated April 27,

2021 filed a claim with the AEPD. The claim is directed against the INSTITU-

NATIONAL TOTAL OF SOCIAL SECURITY with NIF Q2827002C (hereinafter,

INSS). The grounds on which the claim is based are as follows:

THE CLAIMING PARTY states that, together with his partner, he requested the benefit

of

paternity/maternity before the INSS and on March 17, 2021, the INSS sent him a

email in which the correction of the request was required.

Said mail was sent to an incorrect address that does not belong to the claimant.

Along with the claim, provide a copy of the email sent by the INSS (...).

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 INSS, so that it could proceed

give its analysis and inform this Agency within a month, of the actions

carried out to comply with the requirements set forth in the protection regulations

data tion.

The transfer was sent on May 20, 2021 through the Notification Service-

Electronic Information and Electronic Address Enabled, being notified that same

day.

THIRD: On July 20, 2021, and in accordance with the provisions of art.

65 of the LOPDGDD, the admission for processing of the claim filed by

THE CLAIMING PARTY.

FOURTH: On July 26 and 30, 2021 respectively, they are received at the AEPD

two notifications from the INSS, one of them initial and another additional, communicating the breach

of security suffered as a consequence of the remission of personal documentation of

an interested party to a third party.

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

prior investigative actions to clarify the facts in question.

tion, by virtue of the investigative powers granted to the supervisory authorities

in article 57.1 of Regulation (EU) 2016/679 (General Protection Regulation

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

Chapter I, Second Section, of the LOPDGDD, having knowledge of the following-

end tees:

Regarding the chronology of events. Actions taken in order to minimize

adverse effects and measures adopted for their final resolution

□

(…)

Regarding the causes that made the gap possible

(…)

Regarding the measures to be implemented

□

(…)

SIXTH: On March 21, 2022, the Director of the Spanish Agency for

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

for the alleged infringement of article 5.1.f) of the RGPD and article 32 of the RGPD,

typified in articles 83.5 and 83.4 of the RGPD, respectively.

SEVENTH: Notification of the aforementioned start-up agreement in accordance with the established rules

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

Public Administrations (hereinafter, LPACAP), the respondent filed a written

of allegations that, in summary, stated that "... like the rest of the

management entities and common services that make up the Administration of the

Social Security, is subject to the rule that approves and periodically reviews the

Security Committee of Social Security Information Systems

(CSSISS), in the rules of safe use of the information systems of the

Social Security (the latest version of these is attached) ... there is a document

express reference to the use of corporate email by officials

assigned to the Social Security Administration, and a special zeal in terms of

the security measures designed and implemented by the Information Technology Management

of the Social Security, in charge of treatments for the purposes of the systems

computers, to safeguard the integrity, confidentiality, availability and

traceability of systems, including corporate mail, measures that have been

revised and updated after the recent cyberattacks on the servers

IT specialists from different departments of the AGE, as has been the case of the Ministry

of Inclusion, Social Security and Pensions…"

Although it is true that the INSS, as the data controller, is

obliged to apply the appropriate technical and organizational measures to guarantee a

level of security appropriate to the risk presented by the data processing, said

measures are not only measures of computer systems but also measures of

human factor organisations.

It is evident that the security measures implemented were insufficient; Since the

existence of that express document referring to the use of corporate email

by the officials, did not prevent the INSS from sending (***EMAIL.1) a

email to an incorrect address that did not belong to the claimant, in the

that the personal data of the claimant were included: Name and Surname, DNI,

telephone, email address, province and postal code.

In this sense, the INSS provided more information, in order to assess the

possible existence of prior security measures in relation to programming

training of workers.

Emphasizing by this Agency, that the training of public employees

who have access or availability to personal data available in their databases

data is an essential control that every diligent organization must be able to accredit and not

just mention.

Reference was also made by the INSS that, within the programming

training agreement agreed at the social dialogue table with the most

representatives of the workers, has established the provision of two types of

data protection courses, one to be carried out by the provincial directorates,

and another organized by the general management; although, this measure comes to reinforce the

technical and organizational measures in place at the time of the data breach

security.

The INSS in its statement of allegations stated verbatim that "...although it is true

which is an obvious example of the loss of confidentiality of information, it is not

the integrity and availability of the systems and services of the

treatment, since the personal data sent in the email, already

were included in the corresponding computer application as well as in the servers

computer systems of the entity (with the security measures established by the Center

National Cryptologic CCN-CERT and the requirements of the National Scheme of

Security) .

It is evident that in the present case, there is a data security breach

personal data, categorized as a breach of confidentiality, having been referred

by the INSS (***EMAIL.1) an email to an incorrect address that does not

belongs to the claimant, which includes personal data of the claimant:

Name and Surname, DNI, telephone, email address, province and code

Postcard.

When the initiation agreement says "...The referral to the email address

email from a third party of the documentation corresponding to an application of the

birth benefit, so that the interested party can correct its defects,

does not guarantee the confidentiality, integrity and availability of the systems and services

of the treatment…", we were referring to the obligation of the person in charge and of the

in charge of the treatment to apply the appropriate technical and organizational measures

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

among others: b) the ability to guarantee the confidentiality, integrity,

permanent availability and resilience of treatment systems and services.

Finally, the INSS in its allegations referred to the lack of personnel and the

exponential increase in assigned workload; although, that the incident was

due to human error, to the overload of work that has been supporting the

administration, as well as the limitation of human resources, in no case,

justify the violation of the confidentiality, integrity and availability of the

treatment systems and services as well as non-compliance with current regulations

in terms of data protection as responsible for data processing.

EIGHTH: On May 17, 2022, a resolution proposal was formulated,

proposing that the INSS be sanctioned for an infraction of articles 5.1.f) of the

RGPD and 32 of the RGPD, typified in articles 83.5 and 83.4 of the RGPD with a

WARNING for each of the two infractions.

The proposed resolution was notified through the Electronic Notification Service.

cas and Enabled Electronic Address, being notified that same day May 17.

NINTH: On May 31 of that same year, the INSS presented allegations to

the notified motion for a resolution.

PROVEN FACTS

FIRST: It is proven that the INSS sent THE CLAIMING PARTY a copy

e-mail in which he was required to correct the paternity petition /

previously requested maternity.

SECOND: It is proven that said email, (...), was sent to a di-

incorrect action that does not belong to the claimant.

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.”

II

Previous questions

In the present case, in accordance with the provisions of article 4.1 of the RGPD, it consists

carrying out personal data processing, whenever the INSS performs,

among other treatments, the collection, registration, conservation of personal data of the

affiliates such as name, surnames, identification number, address, etc.

III

Allegations adduced

In relation to the allegations presented to the INSS resolution proposal, it was

proceeds to answer them in the order shown.

FIRST. – –The National Social Security Institute (INSS) is
fully committed to complying with current regulations in
matter of protection of personal data and with the principle of responsibility
proactive, which governs the actions of this Administration.
Prior to the incident that gave rise to the proposal for
resolution of sanctioning procedure to this Entity, the INSS had already
conducted an information campaign on the detection and communication of
security breaches (July 2020), which is currently still published
on the institutional intranet (Annex I).
On an annual basis, the INSS has been conducting training courses on
of data protection, where the concept of breach is specifically developed
safety and awareness of the importance of measures
preventive measures (Annex II).
Likewise, a training session on these concepts is given to
newly hired officials. As an accrediting example, we enclose the
training program given in February 2021 to officials of the
Social Security management body, as well as the one given in May
2022 to the officials of the superior body of Technicians of the administration of
Social Security (Annex III).
In this sense we must mention that, not only in INSS but the entire Administration
Public must be fully committed to complying with the regulations in
matter of personal data protection.
The Public Administrations act as data controllers of
personal character and, on some occasions, they exercise functions of those in charge of
treatment, for what corresponds to them, following the principle of responsibility
proactively, meet the obligations that the regulations on data protection

personal imposes on them.

The INSS insists on training aimed at officials of the management body of the

Social Security.

The INSS, as the data controller, is obliged to apply the

appropriate technical and organizational measures to ensure a level of security

appropriate to the risk presented by the data processing.

Within these mandatory technical and organizational measures,

finds the training of public employees who have access or availability to

personal data available in its databases.

Consequently, the programming in formation to which reference is made comes to

strengthen the technical and organizational measures in place at the time of occurrence

the security breach.

SECOND. –. This Institute has continued to adopt various measures in

Data Protection matter:

Multiple awareness actions, publications,

instructions, training actions, development of reference material...

It is worth mentioning the recent institutional objective (from the second half of

2021), which consisted of carrying out a communication action aimed at the entire

INSS personnel, through the provincial directorates, to inform and

raise awareness about the concept of a security breach and the need to

communicate it to the Subdelegate for Data Protection of the INSS. (Annex IV).

As for the specific measures adopted to try to avoid this type of events and make process managers aware of the importance of reviewing recipients of the communications, as well as their correspondence with the documentation or information that contains personal data and that is sent abroad, this Entity has prepared and disseminated an informative pill which is currently published on its corporate intranet (Annex V).

On the other hand, and as a consequence of the process of continuous updating of the action procedures carried out by the INSS, taking advantage of the technical possibilities available at all times and, safeguarding the privacy and safe use policies, in accordance with 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 processing of personal data and the free circulation of these data; and the Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of the digital rights (LOPDGDD), the processes in which it is possible to avoid the intervention of the human factor so that they are developed in an automated way and reduce, as far as possible, the chances of these human failures.

In this regard, it should be noted that recently, the automation of most of the communications issued by this Institute, so that the notifications to be communicated to the citizens have been centralized in the printing press available to the Informatics Management of the Social Security (common support service to the INSS). In this way, it is carried out centrally, through the computer applications of

management used in the processing of their benefits, both the printing

such as the enveloping of communications issued by addresses

provincial offices of the INSS, as well as by their respective Attention Centers and

Information (CAISS), without direct intervention of personnel assigned to this

entity (SARTIDO printing train-INSS document manager), with the

consequent decrease in the probability of errors occurring

humans.

In this sense, we must emphasize that the aforementioned measures will allow said

public body reinforce and have technical and organizational measures

appropriate to guarantee the level of security appropriate to the risk presented by the

data treatment.

At the time of the security breach, it has been proven in the

file that the INSS did not have reasonable security measures based on

of the possible estimated risks.

THIRD. – Taking into account the aphorism “Errare humanum est”, we can point out

that it has been a specific human error on which this Entity has already

adopts a multitude of both preventive and remedial measures. Nevertheless,

the eventual production of these isolated events is unfortunately

inevitable since it is consubstantial to the essence of the human being. Nevertheless,

As has been pointed out, the INSS works permanently in the adoption of

new automation processes to minimize the production of

this type of event.

The INSS insists that the incident was due to human error; although, that the

out due to human error, the overload of work that has been bearing

administration, as well as the limitation of human resources in any case, justifying

can breach the confidentiality, integrity and availability of the systems and

treatment services.

Emphasizing that the automation of procedures will make it possible to reinforce and

with reasonable security measures based on the estimated possible risks.

two, minimizing human error.

QUARTER. – No new security breaches are expected

as a result of this particular incident.

Given the measures achieved, new security violations such as

consequence of this incident.

Although, at all times, we are talking about a forecast, a fact that can

yield or not

This circumstance does not distort the events that occurred or the violation of the

data protection violation committed.

The INSS is accused of committing an infraction for violation of article 5.1.f) of the

GDPR

IV

Article 5.1.f) “Principles related to treatment” of the RGPD establishes:

"1. The personal data will be:

(…)

f) processed in such a way as to guarantee adequate security of the personal data.

personal data, including protection against unauthorized or unlawful processing and against

accidental loss, destruction or damage, through the application of technical measures or

appropriate organizational structures (“integrity and confidentiality”).”

The

infringement

figure

referenced in the

GDPR,

article 83:

“The infractions of the following dispositions will be sanctioned, in accordance with the

section 2, with administrative fines of a maximum of EUR 20,000,000 or, treating-

of a company, of an amount equivalent to a maximum of 4% of the volume of

Total annual global business of the previous financial year, opting for the one with the highest

amount:

a) the basic principles for the treatment, including the conditions for the consent

lien pursuant to articles 5, 6, 7 and 9; (…)”

In this regard, the LOPDGDD, in its article 71 "Infringements" 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 are contrary to

ries to this organic law”.

For the purposes of the limitation period, article 72 “Infringements considered very serious”

you see” of the LOPDGDD indicates:

"1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679,

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:

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

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

In the present case, it has been proven that the personal data of the REFERRED PARTY

CLAMANTE, contained in the INSS database, were unduly disclosed

to third parties, violating the principle of confidentiality; although, it appears in the experience

tooth the communication sent to that third party who had mistakenly received the document

disclosure of the above, with express indication of the prohibition of using the information

erroneously facilitated, and the administrative, civil and criminal consequences that

It would be wrong to breach this prohibition.

The INSS is accused of committing an infraction for violating article 32 of the

GDPR.

SAW

Article 32 “Security of treatment” of the RGPD establishes:

"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 guarantee the confidentiality, integrity, availability and re-

permanent silence of treatment systems and services;

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

promptly 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

I lie.

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

the Member States".

The infringement is referenced in the RGPD, article 83.4 of the RGPD that under the heading

ca "General conditions for the imposition of administrative fines" provides:

"The infractions of the following dispositions will be sanctioned, in accordance with the

section 2, with administrative fines of a maximum of EUR 10,000,000 or, treating-

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

Total annual global business of the previous financial year, opting for the one with the highest

amount:

5)

the obligations of the person in charge and the person in charge in accordance with articles 8,

11, 25 to 39, 42 and 43; (…)”

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

10/12

In this regard, the LOPDGDD, in its article 71 "Infringements" establishes that "Consti-

The acts and behaviors referred to in sections 4, 5 and 6 are infractions

of article 83 of Regulation (EU) 2016/679, as well as those that are contrary to

this organic law”.

For the purposes of the limitation period, article 73 “Infringements considered serious”

of the LOPDGDD indicates:

“Based on the provisions of article 83.4 of Regulation (EU) 2016/679, it is con-

they are considered serious and the infractions that suppose a vulnerability will prescribe after two years.

substantial portion of the items 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.

In the present case, it has been proven that, at the time of the breach

security, there is no evidence that the INSS had reasonable security measures

based on the possible estimated risks.

The INSS states that the incident could have been due to human error (the official

who forwarded the email to the third party, attempted to substitute the email address

previous, whose object or content was very similar, despite having copied the

correct email address, or you did not press “enter” or “paste”

to add it in the recipient section, or, if you pressed it, the program

computer did not replace the old address with the new one, so the

incorrect).

Although the incident was due to human error, the work overload that

has been supporting the administration, as well as the limitation of human resources in

no case, justify the breach of confidentiality, integrity and availability

treatment systems and services.

For the rest, the manner of acting of the official, as described, involves

some risk that errors like this may occur.

Referral to a third party email address for documentation

corresponding to a request for the birth benefit, so that the interested party

correct the defects of the same, does not guarantee the confidentiality, integrity and

availability of treatment systems and services.

Article 83 “General conditions for the imposition of administrative fines” of the

RGPD section 7 establishes:

viii

“Without prejudice to the corrective powers of the control authorities by virtue of art.

Article 58(2), each Member State may lay down rules on whether

of, and to what extent, impose administrative fines on authorities and public bodies

public authorities established in that Member State."

Likewise, article 77 "Regime applicable to certain categories of liability"

responsible or in charge of the treatment" of the LOPDGDD provides the following:

"1. The regime established in this article will be applicable to the treatment of

who are responsible or in charge: …

c) The General State Administration, the Administrations of the communities

Autonomous entities and the entities that make up the Local Administration…

2. When those responsible or in charge listed in section 1 committed

any of the infractions referred to in articles 72 to 74 of this organic law

nica, the competent data protection authority will issue a resolution

sanctioning them with a warning. The resolution will also establish the

measures to be taken to stop the conduct or correct the effects of the

offense that was committed...

3. Without prejudice to what is established in the previous section, the data protection authority

data will also propose the initiation of disciplinary actions when there are in-

Enough words for it. In this case, the procedure and the sanctions to be applied

will be those established in the legislation on disciplinary or sanctioning regime that

result of application.

Likewise, when the infractions are attributable to authorities and managers, and

proves the existence of technical reports or recommendations for the treatment that

had not been duly attended to, in the resolution imposing the

The sanction will include a reprimand with the name of the responsible position and

will order the

publication in the corresponding Official State or Autonomous Gazette.

(…)

5. They will be communicated to the Ombudsman or, where appropriate, to similar institutions

of the autonomous communities the actions carried out and the resolutions issued

under this article. (…)"

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 the NATIONAL INSTITUTE OF SOCIAL SECURITY, with

NIF Q2827002C, for an infringement of article 5.1.f) of the RGPD, typified in the

article 83.5 of the RGPD, a sanction of warning.

IMPOSE the NATIONAL INSTITUTE OF SOCIAL SECURITY, with NIF

Q2827002C, for an infringement of article 32 of the RGPD, typified in the

article 83.4 of the RGPD, a sanction of warning.

SECOND: NOTIFY this resolution to the NATIONAL INSTITUTE OF THE

SOCIAL SECURITY.

THIRD: COMMUNICATE this resolution to the Ombudsman,

in accordance with the provisions of article 77.5 of the LOPDGDD.

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

938-050522

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es