 Procedure No.: PS/00468/2019

938-300320

RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following

BACKGROUND

FIRST: Don A.A.A. (hereinafter, the claimant), dated February 13, 2019,

filed a claim with the Spanish Data Protection Agency. The

claim is directed against Dr. B.B.B. (hereinafter, the claimed).

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

He had a serious accident on July 28, 2017, being admitted to the

Central University Hospital of Asturias, where he was in the U.C.I. and subsequently,

in rehabilitation until March 15, 2018.

The claimant is a civil servant and has arranged medical assistance with Asisa,

who wanted to transfer him to one of their centers for the daily cost of hospitalization in the

Hospital mentioned. On October 19, 2017, they sent an email to his wife

(a copy is attached) indicating that they are going to transfer him to the Covadonga sanatorium in

Gijón, where you will be attended by Dr. B.B.B., who has the reports that have been

facilitated. The transfer did not take place because the doctors at the Hospital did not allow it.

Central University of Asturias, since only there they had means for the

difficult rehabilitation. (Hospital report attached).

Asisa told him that he would pay the cost of the Hospital and changed the

health care to Social Security, through MUFACE, which was aware of the case.

Dr. B.B.B. He is a doctor at the Central University Hospital of Asturias and he was going to

take charge of his rehabilitation at the Covadonga sanatorium in Gijón, in charge of Asisa.

The aforementioned doctor accessed his medical history in July 2017, when he was admitted; but when he was no longer the doctor who treated him, on October 6, 2017, he returned to access your medical record. A few days later he received an email from Asisa informing him of the transfer and the attention of the mentioned doctor.

Report the unauthorized treatment of your health data, data specially protected. He also violated the obligation to inform what he was going to do with your data and the principle of confidentiality.

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 respondent, so that proceed to its analysis and inform this Agency within a month of the actions tions carried out to adapt to the requirements set forth in the regulations of Data Protection.

The Health Service of the Principality of Asturias indicates that it has transferred the I say denounced the claim so that you can allege what you deem appropriate; differing that Service the actions against the physician based on the fact that the Agency Establish whether the accesses are legal or not.

BBB stated the following: that they are statutory staff of (...) at the Hospital Central University of Asturias. He doesn't have any relationship with Asisa, it just happened consultation at the Covadonga Sanatorium on some Thursday afternoons, currently it doesn't. He explains that the first access to his clinical history, upon admission, occurred at

seek help from the doctor who treated you, due to her experience.

The access that occurred on October 6, 2017 is due to the interest of the injured

from the point of view of research. The only research project

Hospital in 2014, for urgent attention to spinal cord injuries, a

for your part. The causal mechanism was rare, recovery is seen at very

long term (up to 3 years). This access is protected by article 16.3 of the Law

of patient autonomy.

He did not know that the patient was a civil servant and had a relationship with Asisa. Ade-

more, he is ***SPECIALITY.1, not being able to carry out the rehabilitation treatment in the

Covadonga sanatorium.

THIRD: The claimant, after receiving the response from the denounced doctor, presented

This new writing indicates the following: that the denounced access is that of the 6th of

October 2017, which occurred on the dates that Asisa called his wife indi-

Telling him that he was better and could be transferred. You cannot justify access in the

Law of autonomy of the patient, as if it were a mixed bag, not even in an old pro-

research project, when also in the rehabilitation phase, as the claim-

he pointed out, it no longer corresponds to him because of his specialty. He insists that the access was not

spoiled.

FOURTH: On June 3, 2019, the Director of the Spanish Agency for Pro-

Data Protection agreed to admit the claim filed by the claimant for processing.

FIFTH: On February 19, 2020, the Director of the Spanish Agency for

Data Protection agreed to initiate a sanctioning procedure against the claimant, for the

alleged infringement of article 6.1. of the RGPD, typified in Article 83.5 of the RGPD.

TO: Notification of the start-up agreement, and published in the BOE as it was not possible to

SEX

make the notification, the defendant at the time of this resolution has not pre-

seated in writing of allegations, for which what is stated in article

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

Public Administrations, which in its section f) establishes that in case of non-

arguments within the stipulated period on the content of the initiation agreement, it

may be considered a resolution proposal when it contains a pronouncement

about the imputed responsibility, for which we proceed to dictate Resolution

tion.

SEVENTH: On August 1, 2020, it was agreed to practice the following

tests:

1. The claim filed by

Don A.A.A. and its documentation.

2. Likewise, the Central University Hospital of Asturias is requested to inform us

me the following, within 10 business days:

a) If Dr. B.B.B. presented a research project of the Hospital in the year

2014, for urgent attention to spinal cord injuries.

a) If the Central University Hospital of Asturias approved said draft

research.

b) If so, duration of the investigation, type of patients who

would be included in the research, information provided to participants in

the investigation.

The request was not delivered to its recipient.

PROVEN FACTS

FIRST: The claimant suffered an accident on July 28, 2017, being admitted

at the Central University Hospital of Asturias, where he was in the U.C.I. Y,

subsequently, in rehabilitation until March 15, 2018.

The claimant is a civil servant and has arranged medical assistance with Asisa,

that he wanted to transfer him to one of their centers.

SECOND: On October 19, 2017, his wife received an email from

Asisa (copy attached) indicating that they would transfer the claimant to the sanatorium

Covadonga de Gijón, where Dr. B.B.B. would assist him, who has the reports

that they have provided.

The transfer did not take place because the doctors at the Hospital did not allow it.

Central University of Asturias, since only there they had means for the

difficult rehabilitation. (Hospital report attached).

THIRD: Dr. B.B.B. He is a doctor at the Central University Hospital of Asturias and

would be the doctor who would continue with his rehabilitation at the Covadonga sanatorium in

Gijón, by Asisa. The aforementioned doctor accessed his clinical history in July

2017, when he entered; but when he was no longer the doctor treating him, on the 6th of

October 2017, he accessed his medical records again.

FOURTH: Dr. B.B.B. alleged that the access made on October 6, 2017 was

due to the interest of the injured party from the point of view of the investigation. The only pro

Hospital research project in 2014, for urgent care to injured

medullary was made by him. The causal mechanism was rare, recovery

ration is observed in the very long term (up to 3 years). This access is covered by the

Article 16.3 of the Patient Autonomy Law.

FIFTH: The Health Service of the Principality of Asturias indicates that it has deferred the actions

actions against the physician depending on whether the Agency establishes whether the accesses or they are not.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of Regulation (EU) 2016/679 (General Data Protection Regulation, hereinafter RGPD), recognizes each Control Authority, and according to the provisions of 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), the Director of the Agency Spanish Data Protection is competent to initiate and resolve this process.

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

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:

"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

Law 40/2015, of October 1, on the Legal Regime of the Public Sector, in

its article 26, which includes one of the principles of the sanctioning power, that of the

non-retroactivity, establishes the following:

"1. The sanctioning provisions in force at the time will apply.

of the occurrence of the events that constitute an administrative infraction.

2. The sanctioning provisions will have a retroactive effect insofar as they

vorce the alleged offender or the offender, both in terms of the classification of the infraction

fraction as well as the sanction and its prescription periods, even with respect to the sanctions

pending compliance upon entry into force of the new provision."

In this procedure, the legality of access to the patient's medical history is questioned.

claimant on October 6, 2017, the date on which the LOPD was in force.

However, that Law classified such treatment as very serious, establishing

minimum amounts higher than the RGPD; Therefore, this last rule will be applied.

IV

The RGPD in its article 5, "Principles related to treatment" says that "The

personal data will be:

(<<legality, loyalty and transparency>>)”

a) processed in a lawful, loyal and transparent manner in relation to the interested party

Article 6 of the RGPD, “Legality of the treatment”, specifies in section 1 the

assumptions in which the processing of third party data is considered lawful:

conditions:

"1. The treatment will only be lawful if it meets at least one of the following

a) the interested party gave his consent for the treatment of his personal data-

them for one or more specific purposes;

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

resado is part or for the application at its request of pre-contractual measures

tuales;

c) the treatment is necessary for the fulfillment of an applicable legal obligation.

cable to the data controller;

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

another natural person.

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

public interest or in the exercise of public powers vested in the controller

of the treatment;

f) the treatment is necessary for the satisfaction of legitimate interests per-

guided by the data controller or by a third party, provided that on di-

such interests do not override the interests or fundamental rights and freedoms

mental data of the interested party that require the protection of personal data, in

particularly when the interested party is a child.

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

performed by public authorities in the exercise of their functions.

2. Member States may maintain or introduce more specific provisions

specific in order to adapt the application of the rules of this Regulation with regard to

Regarding the treatment in compliance with section 1, letters c) and e), setting in a way

more precise specific treatment requirements and other measures that guarantee a

lawful and fair treatment, including other specific situations of treatment

under Chapter IX.

3. (…)"

Article 9 of the RGPD establishes the following:

1. The processing of personal data that reveals the origin

ethnic or racial opinion, political opinion, religious or philosophical conviction, or affiliation

trade union membership, and the processing of genetic data, biometric data aimed at identifying

unequivocally identify a natural person, data relating to health or data relating to

you to the sexual life or sexual orientations of a natural person.

2. Section 1 shall not apply when one of the circumstances

following companies:

a) the interested party gave his explicit consent for the treatment of said data.

personal data with one or more of the specified purposes, except when the Law

of the Union or of the Member States provides that the prohibition referred to in

section 1 cannot be lifted by the interested party;

b) the treatment is necessary for the fulfillment of obligations and the exercise

of specific rights of the person in charge of the treatment or of the interested party in the field

of labor law and social security and protection, to the extent that it is so

authorized by the Law of the Union of the Member States or a collective agreement with

under the law of the Member States that establishes adequate guarantees of the

respect for the fundamental rights and interests of the data subject;

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

another natural person, in the event that the interested party is not qualified, physical or legal,

strictly, to give your consent;

d) the treatment is carried out, within the scope of its legitimate activities and with

due guarantees, by a foundation, an association or any other body

non-profit, whose purpose is political, philosophical, religious or trade union, provided

that the treatment refers exclusively to the current or former members of such

organizations or persons who maintain regular contact with them in relation to

for their purposes and provided that the personal data is not communicated outside of them without

the consent of the interested parties;

e) the treatment refers to personal data that the interested party has made manifest.

festively public;

f) the treatment is necessary for the formulation, exercise or defense of re-

claims or when the courts act in the exercise of their judicial function;

g) the treatment is necessary for reasons of an essential public interest, especially

the basis of the law of the Union or of the Member States, which must be proportionate

nal to the objective pursued, respect essentially the right to data protection

and establish adequate and specific measures to protect the interests and rights

fundamentals of the interested party;

h) the treatment is necessary for purposes of preventive or occupational medicine, eva-

assessment of the worker's work capacity, medical diagnosis, provision of health

maintenance or treatment of a health or social nature, or management of health care systems and services.

health and social assistance, on the basis of the Law of the Union or of the States

members or under a contract with a healthcare professional and without prejudice to the

conditions and guarantees contemplated in section 3;

i) the treatment is necessary for reasons of public interest in the field of

public health, such as protection against serious cross-border threats to the

health, or to guarantee high levels of quality and safety of care

healthcare and medicines or medical devices, on the basis of the Right of

the Union or the Member States establishing appropriate and specific measures

to protect the rights and freedoms of the interested party, in particular the professed secrecy

sional,

j) the treatment is necessary for archiving purposes in the public interest, information purposes,

scientific or historical research or statistical purposes, in accordance with article 89,

paragraph 1, on the basis of the law of the Union or of the Member States, which

must be proportional to the objective pursued, respect essentially the right to

data protection and establish adequate and specific measures to protect the

interests and fundamental rights of the interested party.

3. The personal data referred to in section 1 may be processed for the purposes

cited in section 2, letter h), when their treatment is carried out by a professional

subject to the obligation of professional secrecy, or under your responsibility, in accordance

with the Law of the Union or of the Member States or with the established rules

by the competent national bodies, or by any other person also subject to

also to the obligation of secrecy in accordance with the Law of the Union or of the States.

two members or of the standards established by the competent national bodies.

you.

4. Member States may maintain or introduce additional conditions,

including limitations, with respect to the processing of genetic data, biometric data,

cos or data relating to health.

The facts denounced are specified in the access by the defendant to the

claimant's medical history without any legitimizing cause for it; adding that

that access was used to report it to the medical insurance company of the

claimant, who sent him an email informing him of his transfer to a concerted center

by the company, where he would be attended by the claimed.

The claimant alleges that his access on October 6, 2017 was due to the

interest of the injured from the point of view of the investigation, since he had piloted

a research project of the Hospital in 2014, for urgent attention to

spinal cord injuries whose recovery is observed in the very long term (up to 3 years).

It adds that this access is protected by article 16.3 of the Law of autonomy of the

patient

Law 41/2002, of November 14, regulating patient autonomy

and rights and obligations regarding information and clinical documentation, in

its article 16 dedicated to the uses of clinical history, provides:

"1. The clinical history is an instrument fundamentally destined to

ensure adequate patient care. The healthcare professionals of

center that performs the diagnosis or treatment of the patient have access to the medical history of the latter as a fundamental instrument for adequate assistance.

2. Each center will establish the methods that make it possible at all times to access to the clinical history of each patient by the professionals who assist him.

3. Access to clinical history for judicial, epidemiological, health purposes public, research or teaching, is governed by the provisions of the legislation in force regarding the protection of personal data, and in Law 14/1986, of 25 April, General Health, and other rules of application in each case. access to the clinical history for these purposes requires the preservation of personal identification data of the patient, separated from those of a clinical-assistance nature, so that, as general rule, anonymity is ensured, unless the patient himself has given your consent not to separate them.

The cases of investigation foreseen in section 2 of the Seventeenth additional provision of the Organic Law on Data Protection Personal and Guarantee of Digital Rights.

Likewise, cases of investigation by the judicial authority are excepted. in which the unification of the identification data with the clinicoassistantial ones, in which the judges and courts in the corresponding process. Access to data and documents of the clinical history is strictly limited to the specific purposes of each case.

When this is necessary to prevent a serious risk or danger to the health of the population, the health administrations referred to in the Law 33/2011, of October 4, General of Public Health, will be able to access the data identification of patients for epidemiological reasons or protection of the public health. Access must be carried out, in any case, by a health professional subject to professional secrecy or by another person also subject to an obligation

equivalent of secrecy, prior motivation by the Administration requesting

access to data.

4. The administration and management staff of health centers can only

access medical record data related to their own functions.

5. Duly accredited health personnel who perform health care functions

inspection, evaluation, accreditation and planning, you have access to the histories

clinics in the fulfillment of their functions of verifying the quality of the

assistance, respect for the rights of the patient or any other obligation of the

center in relation to patients and users or the Health Administration itself.

6. The personnel who access the data of the clinical history in the exercise of

its functions is subject to the duty of secrecy.

7. The Autonomous Communities will regulate the procedure so that it remains

proof of access to the medical record and its use."

v

The Hospital Center in which the claimant was admitted and in which

the claimed service provides, it must have incorporated the security measures

adequate for the personal data to be treated in such a way that it is

ensures adequate security of personal data, including the protection

against unauthorized or unlawful processing and against loss, destruction or damage

accidental, through the application of appropriate technical or organizational measures

("integrity and confidentiality").

Article 32 of the RGPD establishes these security measures in the sense

Next:

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

of the 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.

It has been accredited that the requested Hospital has a control of

access that identifies the users, date and time, who accessed the clinical history

of the claimant.

It can be concluded, therefore, that in the present case the information system that

manages the medical history of the Hospital claimed complies with the measures of

security related to access control.

On the other hand, article 70 of the LOPDGDD establishes who is responsible

of breaches of data protection regulations, indicating:

“They are subject to the sanctioning regime established in the Regulation (EU)

2016/679 and in this organic law:

a) Those responsible for the treatments.

b) Those in charge of the treatments.

c) The representatives of those responsible or in charge of the treatments do not

established in the territory of the European Union.

d) Certification entities.

e) The accredited entities for the supervision of codes of conduct…”

The doctor against whom the claim has been filed does not have the consideration

of none of the responsible parties to whom an infringement can be attributed. Hospital

Central University of Asturias must evaluate if it is access made by the doctor

claimed was legitimate, based on the statements made by the same,

referring to their participation in the 2014 Hospital research project,

the possible inclusion in it of the data of the claimant, or to article 16.3 of the

LAP; or initiate disciplinary proceedings if the access was not legitimate and justified

on October 6, 2017.

Therefore, in accordance with the applicable legislation,

The Director of the Spanish Data Protection Agency RESOLVES:

FIRST: FILE the sanctioning procedure initiated against Don B.B.B., as he was not

responsible for the claimed infringement.

SECOND: NOTIFY this resolution to Don B.B.B., the claimant and the Host.

Central University Hospital of Asturias.

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

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 LPA-

CAP, the interested parties may optionally file an appeal for reconsideration before

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

counting from the day following the notification of this resolution or directly

contentious-administrative case before the Contentious-administrative Chamber of the Au-

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 Jurisdiction

Contentious-administrative diction, within a period of two months from the day following

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 LPA-

CAP, the firm resolution may be provisionally suspended 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 city

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

certifying the effective filing of the contentious-administrative appeal. Yes

the Agency was not aware of the filing of the contentious-administrative appeal

nistrative within two months from the day following the notification of the pre-

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