 File No.: PS/00587/2021

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: On November 22, 2020, A.A.A. (hereinafter, the part

claimant) filed a claim with the Spanish Data Protection Agency.

The claim is directed against the MINISTRY OF COMMUNITY HEALTH

DE MADRID, with NIF S7800001E, (hereinafter, the claimed party).

The complaining party states that, on May 16, 2020, it filed a

complaint to the Directorate of the University Hospital of La Paz where he worked, for

the alleged improper access to his medical history by a colleague

work B.B.B. and that he has only received a response that his transfer was made

claim to the Medical Department of Hospital La Paz for investigation.

It indicates that on May 13, 2020, at around 8 a.m., the aforementioned

nurse, from the operating room service in the general building of the University Hospital la

Paz de Madrid, taking advantage of her status as a nurse and using her passwords

personal access, entered, without any care relationship, in his

clinical history, located in the "HCIS computer system" database.

He states that on the same day, May 13, 2020, he reported the facts described to the

nursing supervision of the operating room service where the nurse worked, as well as

as well as the Nursing Department of Hospital la Paz.

Provides a letter dated 05/20/2020, where the head of the Information Service of the

Hospital Universitario La Paz notifies the claimant of the transfer to the Directorate

Medical center of the notification about "improper access to your medical record" and the

claim filed with Salud Madrid.

SECOND: In accordance with article 65.4 of Organic Law 3/2018, of 5

December, Protection of Personal Data and Guarantee of Digital Rights

(hereinafter LOPDGDD), said claim was transferred to the claimed party,

to proceed with its analysis and inform this Agency within a month,

of the actions carried out to adapt to the requirements established in the

data protection regulations.

This Agency does not contain a response to the transfer of the claim.

THIRD: On April 26, 2021, in accordance with article 65 of the

LOPDGDD, the Director of the Spanish Data Protection Agency agreed

admit for processing the claim presented by the claimant.

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

of previous investigative actions to clarify the facts in

matter, by virtue of the investigative powers granted to the authorities of

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

Data Protection, hereinafter GDPR), and in accordance with the provisions of the

Title VII, Chapter I, Second Section, of the LOPDGDD, being aware of the

following extremes of the claimed party:

DEPARTMENT OF HEALTH OF THE COMMUNITY OF MADRID, with NIF S7800001E,

with address at C/ MELCHOR FERNÁNDEZ ALMAGRO, No. 1 - 28029 MADRID

(MADRID).

On 05/24/2021, information is required from the party claimed under the

present investigation file. Not receiving an answer, the

request, receiving a response with the following results:

About access.

A copy of the record of access to the Hospital information system has been requested

of La Paz on 05/13/2020 where the accesses made by the nurse are recorded

cited by the claimant. It is requested to provide the date and time of the accesses, the details of the

type of data accessed, as well as supporting documentation of the justification

tion existing for said accesses.

In view of this, the claimed party only indicates that the Hospital Universitario La Paz has

conducted an investigation into the facts and has concluded that there have been accesses

by the nurse cited by the claimant, in the time slot in which

She goes to the ER at 3:46 a.m. until you are discharged the same day at

10:12 a.m.

About investigations of accesses.

A copy of the appropriate investigations mentioned in the report has been requested.

document from the Patient Care Service, as well as the final response issued

to the claimant, attaching to the request of this Agency a copy of the document

provided by the claimant where the Head of the Information Service of the Hospital

Universitario La Paz communicates the transfer to the Medical Directorate of the center of the

notification about "improper access to your medical record" so that "proceed to

carry out the appropriate investigations".

In this regard, the claimed party indicates that the Hospital de la Paz has carried out

the appropriate investigations to clarify the facts described by the complainant.

They do not provide a copy of the required investigations. Provide a copy of a letter

dated 12/18/2020, indicating that it is the final response sent to the claimant, in

in which the Hospital indicates that the Management will not contact it because "it

an audit is carried out and the appropriate actions are taken, but this does not entail

that the interested party be informed".

They indicate to this Agency that the aforementioned Hospital has a protocol according to which "if

undue access has occurred, it must be assessed by the Committee for the Protection of

Data (PD) what information would be given to the interested party, always informing him that the

right granted to it by the LOPD itself would only cover the

knowledge of the information submitted to treatment, but not which persons, within

within the scope of the organization of the person responsible for the file have been able to access

said information".

They attach the aforementioned protocol entitled Audits to verify compliance in the

accesses to HC (Clinical History), whose copy works in the present actions of

inspection.

Regarding the actions taken in order to minimize the adverse effects and for the

final resolution of the incident.

In this regard, they provide a report from the La Paz Hospital detailing the sequence

of the facts, as well as a copy of the reports of the Nursing Department.

In one of these reports from the Nursing Directorate of the La Paz Hospital, it states:

"On Thursday, May 13, […the claimant…] requests a meeting with me to

inform me of an event that has occurred and that I, as Supervisor of the

Unity, be knowledgeable. He spent the night in the emergency room because, while

duty in the operating room, begins with […]. During his stay in the emergency room, he receives a WhatsApp from a colleague of hers from the operating room where she literally says "the plate is fine". [...the claimant...] responds "how do you know? have you looked at my Clinic history? His partner replies that he has indeed consulted it in his story, apologizing to him right then and there.

[...the claimant...]refers that this act seriously violates her privacy and that this compañera (I quote words verbatim) "has been making life impossible for her for 3 years, and this is the straw that breaks the camel's back".

Seeing the seriousness of the matter, I notify my Area Deputy and [...the claimant...] expresses its wish that these facts do not go unpunished.

Likewise, we spoke with the colleague who has entered the clinical history immediately admitting his mistake and repeatedly apologizing.

He expressed his desire to speak to [...the claimant...] and apologize. Once discussed with the two parties involved and, at the request of [...the claimant...], informs you of the ways available in the hospital to make the claims that deem appropriate. He is also told that his partner is interested in apologize to you personally for consulting your Story without your permission, and in case at any point in your professional relationship you have felt wronged by your attitude towards her."

Regarding the measures adopted to prevent similar incidents from occurring, dates of implementation and controls carried out to verify its effectiveness.

They only mention again the protocol of Verification Audits of the

compliance in the accesses to HC (Medical Record) of edition date on

03/23/2021, indicating that it can be seen in section 4 (Development), a

process of reactive and proactive audits, the latter being monthly

and following a specific structure and follow-up, to meet the requirements of

the Ministry of Health in case of improper access to medical records.

Regarding the security of existing personal data processing with

prior to the facts.

It has been requested to detail the technical and organizational measures adopted to guarantee

a level of security appropriate to the risks detected in relation to access

by health personnel to the clinical records of patients and the Policy of

security adopted by the entity in relation thereto.

They mention in this regard that, in the Security Policy of the Ministry of Health,

a copy of which they provide includes a "Decalogue of good practices for users of

information systems of the Ministry of Health" which is mandatory

compliance for all personnel who provide services in the Ministry (article

12.2).

Regarding the duty to respect data privacy, among other obligations, in

The Decalogue establishes the following:

- Users must access, exclusively, the information necessary for the de-

development of the functions of its activity and only to which it is authorized

(3.1).

- When accessing this information, users are obliged to comply with all measures

security measures established by the regulations on data protection, and other re-

Applicable requirements in accordance with the rules and procedures established in the CSCM

(3.2).

- All persons involved in any phase of the data processing of

personal nature are bound by professional secrecy with respect to these (3.3).

They indicate that the aforementioned Security Policy contemplates that "Failure to comply with

any of the behavior guidelines contained in this Decalogue of

good practices may give rise to the corresponding disciplinary responsibility, if

to do so, in application of the regulatory norms of the legal regime

own disciplinary of the user".

They state that the La Paz University Hospital has a series of measures

established in order to maintain and consolidate the security of information and

privacy, such as the preservation of access traces and the performance

periodic training for staff.

FIFTH: On January 3, 2022, the Director of the Spanish Agency for

Data Protection agreed to initiate disciplinary proceedings against the claimed party,

in accordance with the provisions of articles 63 and 64 of Law 39/2015, of October 1,

of the Common Administrative Procedure of Public Administrations (in

hereinafter, LPACAP), for the alleged infringement of article 5.1.f) of the GDPR and article

32 of the GDPR, typified in articles 83.5 and 83.4 of the GDPR, respectively.

The startup agreement was sent, in accordance with the rules established in the Law

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

Public Administrations (hereinafter, LPACAP), by means of electronic notification,

being received on January 5, 2022, as stated in the certificate that works

on the record.

SIXTH: Once the initiation agreement was notified, the claimed party submitted a written allegations in which, in summary, he stated:

-that the Hospital Responsible for Data Treatment, Hospital Universitario La Paz (HULP), conducted an investigation into the facts, concluding after it that there were improper accesses to your medical record during the interval in which the complainant was in the ER (3:46 a.m. until 10:12 a.m. of the same discharge date: June 13, 2020),

-That there are adequate and sufficient security measures for the management of Clinical Histories, every time the activities of the users are recorded, retaining the information needed to monitor, analyse, investigate and document improper or unauthorized activities, allowing the identification at all times of the person acting, counting the center with a protocol established for such purposes, in which includes a process of reactive and proactive audits, the latter being on a monthly basis and following a specific structure and follow-up, to attend to the requirements of the Ministry of Health in case of improper access to medical records,

-that they have a Security Policy at the level of the Ministry of Health, which provides specific organizational measures for the maintenance of confidentiality of the information accessed by the workers of the organization,

-that in the medical records management system there is a segregation of profiles for the use of the tool, based on the performance of the work of each of positions.

The document that establishes the assignment of Users and standard profiles is attached, in the which state that: "it can be verified that due compliance is given at the beginning minimum privilege, in accordance with the provisions of Annex II [op.acc.3] of the

National Security Scheme limiting each user to a strictly minimum

necessary to fulfill its obligations. In addition, the privileges are limited in a way

that users only access information necessary for the fulfillment of their

functions.

Therefore, there are different user models defined, such as:

• Administrative User

• Medical User (one per specialty)

• Nursing user (midwives, supervisors, nurses)

• Query User (only gives access to see the information, but does not allow registration)

• User for other non-medical groups

The user models are made up of different profiles, and each profile

allows access to certain functions or powers, always having

present that, according to Law 41/2002, of November 14, basic regulation of the

patient autonomy and rights and obligations in terms of information and

clinical documentation, in its article 16 it is indicated that the clinical history is a

instrument intended primarily to ensure adequate assistance to the

patient, that is, the clinical history must be accessible in such a way that it can be

ensure that adequate care is provided to each patient, taking into account

the diversity of health professionals existing in the center. For example, in the

cases of emergencies, this medical history must be accessible to ensure the

vital interests of every citizen.

When a professional joins the center, they are assigned the model user

established, but if the professional changes their functions or requires new functions,

must have the approval of the Directorate. In the event that a user claims

new functions and there is no established model user, Management values the

relevance of creating a new model user.

Thus, and as we can see in the protocol, there are no generic users,

but rather, they are users created according to the functions they have

assigned, being the univocal and nominal access for each professional with their number of

Personal ID."

-that they have signed a Confidentiality Commitment, through which they

informs the worker at the time of formalizing his contract with the hospital, about the

mandatory security and privacy policies for employees of the

Hospital,

-that training is provided regarding the security of personal data

staff,

-that the claimed party acknowledged its error and apologized to the claiming party,

indicating the lack of intentionality when accessing your information, from what they understand

that security measures, both technical and organizational, carried out by

the person in charge of the Treatment, are optimal and valid to guarantee the security and

confidentiality of patient data.

SEVENTH: On March 11, 2022, the instructor of the procedure issued

proposed resolution for infringement of the provisions of article 5.1 f) of the GDPR.

The aforementioned resolution proposal was sent, in accordance with the rules established in

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

Public Administrations (hereinafter, LPACAP), by means of electronic notification,

being received on March 12, 2022, as stated in the certificate that works

on the record.

EIGHTH: On March 28, 2022, the respondent entity submitted a written

allegations to the Resolution Proposal, in which, in summary, he stated in relation to

with the established security measures that, in application of the National Scheme

Security, the activities of the users are recorded, retaining the information

information necessary to monitor, analyze, investigate and document independent activities

unauthorized or unauthorized, allowing to identify at all times the person who acted

túa, which have implemented a process of reactive and proactive audits

the latter being of a monthly nature and following a structure and follow-up

concrete, to meet the requirements of the Ministry of Health in case of

improper access to medical records, that there is a segregation of profiles for the

use of the tool, based on the performance of the work of each of the

positions, limiting access to each user to the minimum, which by the employees

two, a Confidentiality Commitment is signed, through which the tra-

downstairs at the time of formalizing his relationship of his duties in this matter and that

an informative box (banner) appears warning that access to the platform

It must be done for healthcare purposes.

And in relation to other considerations, he affirms that the clinical history is an instrument

Fundamentally intended to ensure adequate care for the patient, it is

In other words, the medical history must be accessible in such a way that it can be ensured that it is

provides adequate assistance to each patient, training is given regarding

regarding the security of personal data, that the appropriate in-

investigations, which led to the necessary actions to solve the facts

events occurred, being able to identify at all times the person who made the access

due to history and that the mitigating measures carried out by the Hospital,

According to the request of the affected party, they have consisted of a warning

Finally, it mentions the Disciplinary procedure of the AEPD Procedure Nº:

AP/00056/2014. In said resolution issued on February 9, 2021, the AEPD had

opportunity to rule on possible improper and unjustified access to history

clinic of a worker patient of the Madrid Health Service. The AEPD, affirms the

concerned, would have reached the conclusion that SERMAS had established

sufficient security measures.

NINTH: In view of the facts considered proven and in accordance with the

powers that article 58.2 of Regulation (EU) 2016/679 (General Regulation of

Data Protection, hereinafter GDPR), grants each control authority and according to

the provisions of articles 47 and 48.1 of Organic Law 3/2018, of December 5,

Protection of Personal Data and guarantee of digital rights (hereinafter,

LOPDGDD) and in use of the power provided for in article 90.2 of Law 39/2015, of 1

October, of the Common Administrative Procedure of Public Administrations,

On August 23, 2022, the claimed party is notified of the consideration of

that, from the proven facts, not only the violation of article 5.1.f) of the

GDPR, but also that of article 32 of the same legal text.

TENTH: Once the Resolution Proposal was notified, the claimed party submitted a written

of allegations in which, in summary, he stated that an adequate provision of the

health care implies the participation of several services of the same center for the

achievement of the ultimate goal of the well-being and health of the patient, which, in fact, in the

health practice, it is common for an emergency service to lead to a

operating room service, in which it would be strictly necessary to preserve the

vital interests of the affected party, that the health personnel of both services have

immediate access to the patient's medical history in order to provide an adequate

emergency health care.

They provide a report issued by the University Hospital of La Paz in which it is indicated, in

relation to the measure proposed by the AEPD that each of the professionals

could have access to the medical records only of those patients on whom

which carry out their activity, that said measure is extremely complex and difficult

to apply both at a technical and organizational level, and above all from the point of view

care, and this because health professionals and especially the area of nursing

Mería, are subject to continuous shift changes; can carry out their activity

on a rotating basis, going from morning shift to afternoon or night. Similarly, and

Regarding the unit, service or medical specialty, criteria could not be applied either.

ries of exclusion since the health personnel can change location. A prof-

professional can carry out their activity in a plant or specialty and the next day

or next turn in a different one.

Therefore, they consider that health personnel should have access to the different

diagnostic tests performed or consult reports from other specialists and/or professionals.

sionals that may influence the pathology being treated. They further add that the

patients can exercise their right to Free Choice of Specialist, Free Choice

Health Center, request one according to opinion or be channeled at optional request

to a different center to carry out a test or treatment not included in the portfolio
service center of origin. In these situations, health professionals,
have to be able to access the patient's complete medical record in order to offer a
adequate care for the sick.

Lastly, they deem it necessary for the profiles of the configuration system to come
configured as they are up to now since it is the best way to pre-
preserve the health of patients who come to the hospital where care is provided
and indicate that there is already a strong segregation of profiles for the use
of the tool, based on the performance of the work of each one of the positions, limited
giving each user access to the minimum.

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: On November 22, 2020, the claimant filed a
claim before the Spanish Agency for Data Protection, for the alleged access
due to her medical history, by a co-worker.

SECOND: The Hospital Responsible for Data Treatment, carried out a
investigation of the facts, concluding after it that there were accesses
undue to her medical history during the interval in which the complainant
was in the ER (3:46 a.m. until 10:12 a.m. of the same day that
is discharged: June 13, 2020).

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."

In response to the allegations presented by the respondent entity to the Agreement of

beginning of the disciplinary procedure, the following should be noted:

II

The GDPR defines, in a broad way, "data security breaches

personal" (hereinafter security bankruptcy) as "all those violations of the

security that cause the destruction, loss or accidental or illegal alteration of

personal data transmitted, stored or processed in another way, or the

unauthorized communication or access to said data."

In the present case, it is clear that there was a data security breach

in the circumstances indicated above, categorized as breach of

confidentiality, as a consequence of exposure to a third party, of the

personal data relating to the health of the complaining party.

Article 32 of the GDPR states the following:

"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) pseudonymization and encryption of personal data

b) the ability to ensure confidentiality, integrity, availability and resilience

permanent treatment systems and services;

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

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and assessment 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 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.

The aforementioned article provides that "the controller and the person in charge of the treatment

apply appropriate technical and organizational measures to ensure a level of

risk-appropriate security. Consequently, it does not adopt a closed relation of

technical and organizational measures, but these must be the appropriate ones in

function of the level of risk previously analyzed.

That said, article 32.1 includes an obligation of means and not an obligation

of result. Indeed, it indicates that "the person responsible and in charge of the treatment applied

Appropriate technical and organizational measures shall be taken to guarantee a level of safety

appropriate to the risk. In other words, it imposes the obligation to establish a level of security

security, and that level must be based on the risk analysis that every person in charge

must carry out in accordance with section 2 of said article:

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

takes into account the risks presented by data processing, in particular as con-

sequence of accidental or unlawful destruction, loss or alteration of data

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

unauthorized access or access to said data."

The technological evolution and sophistication of systems for unauthorized access to systems

data issues means that the regulations cannot unconditionally impose

a total assurance of the absence of breaches of integrity or confidentiality.

But it does require that those responsible for the treatments must carry out an analysis of

risks and the implementation of an "adequate security level" for them.

Therefore, this duty is characterized as an obligation of means. He has so declared

The Supreme Court found in its recent judgment of February 15, 2022:

“The obligation to adopt the necessary measures to guarantee the security

of personal data cannot be considered an obligation of result, which

implies that a leak of personal data to a third party exists

responsibility regardless of the measures adopted and the activity

displayed by the person responsible for the file or treatment.

In obligations of means, the commitment acquired is to adopt

technical and organizational means, as well as deploying a diligent activity

in its implementation and use that tends to achieve the expected result with

means that can reasonably be described as suitable and sufficient for its

achievement, for this reason they are called obligations "of diligence" or "of behavior".

treatment".

The difference lies in the responsibility in both cases, because while

in the obligation of result, responds to a harmful result due to the failure of the

security system, whatever its cause and the diligence used. In the

obligation of means is enough to establish technically appropriate measures and

implement and use them with reasonable care.

In the latter, the sufficiency of the security measures that the person responsible

has to establish has to be related to the state of technology in

at all times and the level of protection required in relation to personal data.

Sonales treated, but a result is not guaranteed. As established by art. 17.1

of Directive 95/46/EC regarding the security of the treatment the controller

of the treatment has the obligation to apply the technical and organizational measures

adequate measures «These measures must guarantee, taking into account the knowledge

existing technical foundations and the cost of application, a level of security

appropriate in relation to the risks presented by the treatment and to the nature

nature of the data to be protected. And in the same sense it is pronounced

nowdays the art. 31 of the European Union Regulation 2016/679, of

Parliament and of the Council on the protection of natural persons with regard to

regarding the processing of personal data and the free circulation of these

data and by which Directive 95/46/EC is repealed, by establishing with respect to the

security of processing than appropriate technical and organizational measures

they are «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 persons

You sound physical […]".

We have already reasoned that the obligation that falls on the person responsible for the file

and on the person in charge of the treatment regarding the adoption of necessary measures.

measures to guarantee the security of personal data is not a

obligation of result but of means, without the infallibility of the

measures taken. Only the adoption and implementation of mea-

technical and organizational measures, which according to the state of technology and in re-

relation to the nature of the treatment carried out and the personal data in

matter, reasonably allow to avoid its alteration, loss, treatment or

Unauthorized access."

Having established the foregoing, that is, that the obligation of means imposed by article 32 of the GDPR consists of adopting security measures in the treatment, tending to avoid the production of a security breach in it. These obligations of- must be established based on the risks that have been analyzed, and taking into account the state of technology at all times and the level of protection required do in relation to the personal data processed.

Accordingly, the analysis should be performed to determine if the in- compliance consists of determining whether the measures were sufficient to prevent address the risk of a security breach. In this case, it should be checked whether the measures were adequate to ensure that unauthorized access to the history did not occur.

clinical history of the claimant such as the one that occurred in this case. This with inde- depending on whether such access actually occurred, or not.

It is necessary to analyze the allegations made in this procedure by the COUNCIL- HEALTH RIVER. In relation to the security measures established:

- In application of the National Security Scheme, the activities are recorded of users, retaining the necessary information to monitor, analyze, investigate and document improper or unauthorized activities, allowing identify at all times the person acting

-

Implementation of a process of reactive and proactive audits, these being latest on a monthly basis and following a specific structure and follow-up,

to meet the requirements of the Ministry of Health in case of access

you are wrong to medical records

- There is a segregation of profiles for the use of the tool, in

based on the performance of the work of each of the positions, limiting each

user access to a minimum.

- The employees sign a Confidentiality Commitment,

through which the worker is informed at the time of formalizing his relationship

tion of their duties in this matter.

- An information box (banner) appears warning that access to the platform

taforma must be performed for healthcare purposes

And in relation to other considerations he states:

-

The clinical history is an instrument fundamentally designed to guarantee

adequate care for the patient, that is, the clinical history must be accessible

in such a way that it can be ensured that adequate assistance is provided.

cia to each patient

- Training is given regarding the security of personal data.

sound

- The appropriate investigations were carried out, which led to the actions

necessary to solve the events that occurred, being able to identify in

at all times the person who made the improper access to the history.

-

The mitigating measures carried out by the Hospital, in response to the request for

the affected, have consisted of a warning

Finally, it mentions the Disciplinary procedure of the AEPD Procedure Nº:

AP/00056/2014. In said resolution issued on February 9, 2021, the AEPD had

opportunity to rule on possible improper and unjustified access to history

clinic of a worker patient of the Madrid Health Service. The AEPD, affirms the

concerned, would have reached the conclusion that SERMAS had established measures

sufficient security days.

In relation to these allegations, the following must be stated:

Of the five security measures described, it can already be ruled out from the outset that

four of them can be effective in preventing unauthorized access. In

In the first place, the registration of accesses or the performance of audits are measures to

react a posteriori, once the access has occurred. Second, the bank

ner has only informative purposes, without preventing the professional from continuing in

if the access was not justified. Finally, the commitment to confi-

dentiality also does not prevent, by itself, unauthorized access.

Only the segmentation of access profiles to medical records could con-

be considered a valid and effective tool for the avoidance of events such as the

case you The MINISTRY OF HEALTH provides a very detailed annex with the profiles

of each of the types of professional category, distinguishing between ad-

ministerial and health, and within this last category, by types and specialties of

staff.

However, a measure that would be basic is not reflected in the document, and that is that

each of the health professionals could have access to the medical records

only of those patients on whom they deploy their care activity.

In this sense, article 16 of Law 41/2002, of November 14, basic regulation

autonomy of the patient and rights and obligations in terms of information

tion and clinical documentation provides that “1. The clinical history is an instrument

primarily aimed at ensuring adequate care for the patient. The prof-

care professionals of the center who carry out the diagnosis or treatment of the patient

patient have access to the patient's clinical history as a fundamental tool for

your proper assistance.

2. Each center will establish the methods that allow access to

the clinical history of each patient by the professionals who assist him” (underlining

is ours).

From reading this precept it is clearly inferred that, although the clinical history is

the instrument to provide health care to the patient, which must remain due to

duly guaranteed, so is the fact that access can only occur

to the clinical history by the professionals who assist you, not in general, but

with a particular character carrying out the diagnosis or treatment of the patient.

Let us remember that the assumption of fact that has given rise to this procedure con-

access by a nursing person from the Operating Room Service

regarding a patient who received medical assistance in the Emergency Department.

It is true that, as the interested party affirms, "the clinical history is an instrument destined

fundamentally to guarantee adequate care for the patient, that is, the

medical history must be accessible in such a way that it can be ensured that it is provided

adequate assistance to each patient", but it is no less so that they can implement-

are measured, depending on the patients assigned to each professional, of the service in

that the sanitary tasks are carried out, and of the work shifts of each professional.

that prevent a professional from accessing medical data related to

aspect of a patient for whom care activity is not entrusted to

guna. The strong segregation of profiles that they say they have implemented has not prevented

giving access to a patient's clinical history, by a nurse who did not

I was entrusted with the treatment of the patient. This indicates the absence of measures

of adequate security.

The lack of adoption of a measure such as the one described means that it cannot be considered

that there are security measures that provide an adequate level of protection

to existing risks. In fact, the MINISTRY OF HEALTH itself recognizes the

illegality of the conduct, since he processed a disciplinary file against

the person who made the improper access, and which concluded with the imposition of a

warning.

In relation to the precedent invoked (exp. AP/00056/2014), it should be noted that

This is a disciplinary procedure that was carried out for very previous events.

res to the entry into force of the GDPR. The latter entered into force in May 2018, while

after the events occurred in May 2013. In said file, it was carried out

carry out a file of actions based on the fact that the MINISTRY OF HEALTH accredited

tó have in practice the measures required by the already repealed Royal Decree 1720/2007,

of December 21, (RLOPD) by which the regulations for the development of the Law are approved

Organic 15/1999, of December 13, Protection of Personal Data.

(LOPD)

The system established by the previous LOPD differs substantially from that established by

the current GDPR. While the former established a system of security measures

legally established (in conjunction with the RLOPD) to be understood

Once the security obligations have been fulfilled, the current GDPR is based on the

principles of proactive responsibility and data protection by design, that is,

in the establishment of the measures that are necessary based on the risks

valued inherent to a certain treatment. There is therefore no number

rus clausus of measures that the data controller must adopt, but rather

These must be established on a case-by-case basis, based on the risk analysis and the

data that is being processed.

In this regard, article 5.2 of the GDPR establishes, after listing the principles

regarding the protection of personal data, the following:

"2. The data controller will be responsible for compliance with the dis-

listed in section 1 and able to demonstrate it ("proactive responsibility")."

And regarding the principle of data protection by design, the GDPR requires:

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

nature, scope, context and purposes of the treatment, as well as the risks of different

great probability and seriousness that the treatment entails for the rights and freedoms

of natural persons, the data controller will apply, both in the

time of determining the means of treatment as at the time of pro-

proper treatment, appropriate technical and organizational measures, such as pseudonymous

mization, designed to effectively apply the principles of protection

of data, such as data minimization, and integrate the necessary guarantees in

processing, in order to comply with the requirements of this Regulation and to protect

the rights of the interested parties

For all these reasons, the reference to the precedent constituted by file AP/00056/2014

it lacks any virtuality, since it was processed under a rarity regulation.

radically different from today.

For the rest, the criteria of the AEPD in relation to this type of unauthorized access

two has a clear precedent, produced in a disciplinary procedure processed

after the entry into force of the GDPR. This is file reference PS/00250/2021,

in which the EXTREMEÑO HEALTH SERVICE was penalized for an identical problem

the one that concerns us in this file. In the narration of the facts it appears:

"Inspection actions begin upon receipt of a claim document.

A.A.A. (hereinafter, the claimant), in which he states that there have been

undue access to his medical history by a worker

of the Extremadura Health Service (hereinafter SES), with professional category

of nurse. The accesses are made without the authorization of the claimant and without

that mediates a relationship that justifies it."

This procedure should conclude with the imposition of two sanctions for these acts.

two: one for the violation of article 5.1.f) GDPR, in the terms explained in

the proposed resolution and another for article 32 of the Regulation. that is the criteria

of this Agency in relation to this type of assumptions.

II

In response to the latest allegations presented by the respondent entity, it should be

point out the following:

First of all, we are dealing with a special category of personal data

(article 9.1 GDPR) to which the principle of prohibition of treatment is applicable,

unless one of the circumstances provided for in section 2 occurs. Therefore,

they incorporate an innate danger, and must be subjected to a higher standard of protection.

high.

Recital 51 provides, regarding the special categories of personal data,

that:

"Special protection deserves personal data that, by its nature, is

particularly sensitive in relation to fundamental rights and freedoms,

since the context of their treatment could entail significant risks for the

fundamental rights and freedoms. […] Such personal data should not be

treated, unless their treatment is permitted in specific situations

covered by this Regulation, taking into account that Member States

Members may establish specific provisions on data protection with

in order to adapt the application of the rules of this Regulation to the

compliance with a legal obligation or the fulfillment of a mission carried out in

public interest or in the exercise of public powers vested in the person responsible for the

treatment. In addition to the specific requirements of that treatment, there must be applied

the general principles and other rules of this Regulation, especially as regards

refers to the conditions of legality of the treatment. They must be established

explicit exceptions to the general prohibition of treatment of these categories

personal data, among other things when the interested party gives his

explicit consent or in the case of specific needs, in particular

when the treatment is carried out in the framework of legitimate activities by

certain associations or foundations whose objective is to allow the exercise of the

fundamental liberties".

It is a priority to determine the role played by the Ministry of Health.

It follows that the person responsible for the processing of the data that is part of the

clinical history is the health center, public or private; they have the obligation to

prepare it, guard it and implement the necessary security measures so that it does not

is lost, not communicated to non-interested parties or can be accessed by third parties

Not allowed.

The GDPR explicitly introduces the principle of liability (article 5.2 GDPR),

that is, the person responsible for the treatment will be responsible for compliance with the

provided for in paragraph 1 of article 5 and must be able to prove it

“proactive responsibility”.

Report 0064/2020 of the Legal Office of the AEPD has emphatically expressed

that "The GDPR has meant a paradigm shift when addressing the regulation of the

right to the protection of personal data, which is based on the

principle of "accountability" or "proactive responsibility" as indicated by

repeatedly by the AEPD (Report 17/2019, among many others) and is included in the

Explanation of reasons for the Organic Law 3/2018, of December 5, Protection of

Personal Data and guarantee of digital rights (LOPDGDD)”.

The requested party, in its capacity as the data controller, should

have adopted and implemented, proactively, the technical and

organizational measures that are appropriate to evaluate and guarantee a level of

appropriate security to the probable risks of diverse nature and severity

linked to the health data processing carried out.

For these purposes, article 24 of the GDPR under the heading "Responsibility of the

responsible for the treatment" provides:

"1. Taking into account the nature, scope, context and purposes of the processing,

as well as risks of varying probability and severity for the rights

rights and freedoms of natural persons, the person responsible for the treatment applied

shall take appropriate technical and organizational measures in order to guarantee and be able to

show that the treatment is in accordance with this Regulation. said

measures will be reviewed and updated when necessary.

2. When provided in connection with processing activities,

the measures referred to in paragraph 1 shall include the application, for

part of the person responsible for the treatment, of the appropriate protection policies

of data. (…)"

For its part, article 25 of the GDPR under the heading "Data protection from the

sign and by default" provides:

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

nature, scope, context and purposes of the treatment, as well as the risks of dif-

versa probability and seriousness involved in the treatment for the rights and

freedoms of natural persons, the data controller will apply, both

at the time of determining the means of treatment as at the time

of the processing itself, appropriate technical and organizational measures, such as the

pseudonymization, designed to effectively apply the principles of

data protection, such as data minimization, and integrate safeguards

necessary in the treatment, in order to comply with the requirements of this Regulation.

ment and protect the rights of the interested parties.

2. The data controller will apply the technical and organizational measures

with a view to ensuring that, by default, they are only processed

personal data that is necessary for each of the purposes

treatment specifics. This obligation will apply to the amount of data

personal information collected, to the extent of its treatment, to its retention period

vation and its accessibility. Such measures shall ensure in particular that, for

defect, the personal data are not accessible, without the intervention of the per-

sona, to an indeterminate number of natural persons. (…)"

Likewise, the LOPDGDD in article 28.1 states that:

"Those responsible and in charge, taking into account the elements enumerated

two in articles 24 and 25 of Regulation (EU) 2016/679, will determine the

appropriate technical and organizational measures that they must implement in order to guarantee

certify and certify that the treatment is in accordance with the aforementioned regulation, with the

this organic law, its development regulations and the applicable sectoral legislation

wire."

Consequently, the responsibility of the data controller must be established.

treatment for any processing of personal data carried out by himself or by

your account. In particular, the person responsible must be obliged to apply opportune measures.

and effective and must be able to demonstrate compliance of processing activities

compliance with the GDPR, including the effectiveness of the measures (GDPR recital 74).

In summary, this principle requires a conscious, diligent, committed and

proactive on the part of the person responsible for all data processing

personal you carry out.

In the present case, the defendant entity is charged with the lack of implementation of

the technical and organizational measures necessary to guarantee a level of security

appropriate to the risk derived from the treatment of patient health data (category
special category of personal data in accordance with the provisions of article 9.1 of the
GDPR), in order to prevent the violation of the principle of confidentiality, as
is clear from the assessment of the set of facts analyzed.
In general, it should be noted that in the treatment of clinical histories it is not
must wait until the improper access has occurred to react later
(which would shift the responsibility to the worker instead of the person responsible for the
treatment) but, based on the aforementioned principles of responsibility
proactive and data protection from the design, prevent improper access
produce.

From the foregoing, it is evident that the defendant, as the person responsible for the ob-
object of study, has not shown the diligence that was required to establish
the security measures that are necessary to avoid the filtration or diffusion of
this type of data to third parties. In this sense, the configuration of technical measures
and organizational processes must be carried out so that, prior to carrying out the
processing of personal data, it is guaranteed that you can only have access to
the stories those personnel who carry out their care activity on the holder of
are.
In the event that the computer application that controls access to medical records
were correctly programmed, it could determine, at the moment in which it was
tenders access, if the person requesting it (according to their specialty, shift or activity in

that moment) must be legitimated to access it.

Lastly, data protection by design must be complemented by implementation.

periodic auditing, so that failures in the system can be detected

which, in turn, recommend modifying the access protocols in case of independent access.

bidos.

Consequently, the allegations must be dismissed, meaning that the

arguments presented do not distort the essential content of the offense that

is declared committed nor does it imply sufficient justification or exculpation.

The requested entity is accused of committing an infraction for violation of the

Article 5.1.f) of the GDPR, which governs the principle of confidentiality and integrity of the

personal data, as well as the proactive responsibility of the data controller

treatment to demonstrate its compliance and article 32 of the GDPR.

IV.

Regarding the health data, recital 35 of the GDPR states the following:

“Personal data relating to health should include all personal data

relating to the state of health of the interested party that provide information about their state of

past, present or future physical or mental health. Information is included about the

natural person collected on the occasion of your registration for the purposes of health care,

or on the occasion of the provision of such assistance, in accordance with Directive

2011/24/EU of the European Parliament and of the Council; any number, symbol or data

assigned to a natural person who uniquely identifies them for the purposes of

sanitary; information obtained from tests or examinations of a part of the body or

of a body substance, including from genetic data and samples

biological, and any information related, by way of example, to a disease, a

disability, disease risk, medical history, treatment

clinical or physiological or biomedical state of the data subject, regardless of their

source, for example a doctor or other healthcare professional, a hospital, a device

physician, or an in vitro diagnostic test.”

For its part, Article 4 of the GDPR defines:

"2) "processing": any operation or set of operations carried out on

personal data or sets of personal data, either by procedures

automated or not, such as the collection, registration, organization, structuring,

conservation, adaptation or modification, extraction, consultation, use,

communication by transmission, diffusion or any other form of authorization of

access, collation or interconnection, limitation, deletion or destruction;”

7) "responsible for the treatment" or "responsible": the natural or legal person,

public authority, service or other body which, alone or jointly with others, determines the

purposes and means of processing; if the law of the Union or of the Member States

determines the purposes and means of processing, the controller or the

Specific criteria for their appointment may be established by Union law

or of the Member States;

10) "third party": natural or legal person, public authority, service or other body

of the interested party, the person in charge of the treatment, the person in charge of the treatment and the

persons authorized to process personal data under the direct authority of the

responsible or of the person in charge;”

The treatment of data from medical records is regulated by Law

41/2002, of November 14, basic regulation of patient autonomy and

rights and obligations regarding information and clinical documentation.

V

Its article 3 states:

"Clinical history: the set of documents that contain the data, assessments and

information of any kind on the situation and clinical evolution of a

patient throughout the care process.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

In article 16, the uses of the clinical history are established:

"1. The clinical history is an instrument fundamentally designed to guarantee

adequate patient care. The healthcare professionals at the center who

perform the diagnosis or treatment of the patient have access to the medical history

of it as a fundamental instrument for its adequate assistance.

2. Each center will establish the methods that allow access to

the medical history of each patient by the professionals who assist him."

SAW

Article 5.1.f) of the GDPR

Article 5.1.f) of the GDPR establishes the following:

"Article 5 Principles relating to treatment:

1. Personal data will be:

(…)

f) processed in such a way as to guarantee adequate data security

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

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

or organizational procedures (“integrity and confidentiality”).”

In relation to this principle, Recital 39 of the aforementioned GDPR states that:

“[…]Personal data must be processed in a way that guarantees security and

appropriate confidentiality of personal data, including to prevent access

or unauthorized use of said data and of the equipment used in the treatment”.

It should be added that, in relation to the category of data to which a third party

someone else has had access, they are in the special category according to what

provided in art. 9 of the GDPR, a circumstance that implies an added risk that is

must be assessed in the risk management study and that the degree requirement increases

of protection in relation to the security and safeguarding of the integrity and

confidentiality of these data.

Consequently, it is considered that the accredited facts are constitutive of

infringement, attributable to the claimed party, due to violation of article 5.1.f) of the

GDPR.

Classification of the infringement of article 5.1.f) of the GDPR

VII

Article 83.5 of the GDPR provides the following:

"5. Violations of the following provisions will be penalized, 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:

to)

the basic principles for the treatment, including the conditions for the

consent in accordance with articles 5, 6, 7 and 9;”

For its part, Article 71 of the LOPDGDD, under the heading "Infractions" determines what

following:

"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 for infringements, article 72 of the LOPDGDD,

under the rubric of offenses considered very serious, establishes the following:

"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.”

VIII

GDPR Article 32

Article 32 of the GDPR, security of treatment, establishes the following:

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

nature, scope, context and purposes of processing, as well as risks of

variable probability and severity for the rights and freedoms of individuals

physical, the person in charge and the person in charge of the treatment will apply technical and

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

which may include, among others:

a) the pseudonymization and encryption of personal data;

b) the ability to ensure the confidentiality, integrity, availability and

permanent resilience of treatment systems and services;

c) the ability to restore availability and access to data

quickly in the event of a physical or technical incident;

d) a process of regular verification, evaluation and assessment of effectiveness

of the technical and organizational measures to guarantee the security of the treatment.

2. When evaluating the adequacy of the level of security, particular attention should be paid 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 said data (The underlining is from the AEPD).

Recital 75 of the GDPR lists a series of factors or assumptions associated with

risks to the guarantees of the rights and freedoms of the interested parties:

“The risks to the rights and freedoms of natural persons, serious and

variable probability, may be due to data processing that could cause

physical, material or immaterial damages and losses, particularly in cases in which

that the treatment may give rise to problems of discrimination, usurpation of

identity or fraud, financial loss, damage to reputation, loss of

confidentiality of data subject to professional secrecy, unauthorized reversal of the

pseudonymization or any other significant economic or social harm; in the
cases in which the interested parties are deprived of their rights and freedoms or are
prevent you from exercising control over your personal data; In cases where the data
personal treaties reveal ethnic or racial origin, political opinions, religion
or philosophical beliefs, union membership and genetic data processing,
data relating to health or data on sexual life, or convictions and offenses
criminal or related security measures; in cases where they are evaluated
personal aspects, in particular the analysis or prediction of aspects related to the
performance at work, economic situation, health, preferences or interests
personal, reliability or behavior, situation or movements, in order to create or
use personal profiles; in cases in which personal data of
vulnerable people, particularly children; or in cases where the treatment
involves a large amount of personal data and affects a large number of
interested."

In the present case, as established in the facts and in the framework of the file
E/05028/2021, the AEPD requested to provide the date and time of the accesses, the details of the
type of data accessed, as well as supporting documentation of the
existing justification for such accesses. In the documentation provided, the
The defendant only acknowledges the existence of said accesses, although he does not pronounce
about the legitimacy of these nor does it provide a copy of the required investigation.

The consequence of this implementation of deficient security measures was the
exposure to a third party of personal data relating to the health of the
complaining party. That is, the affected person has been deprived of control over their
personal data relating to your medical history.

It should be added that, in relation to the category of data to which a third party
someone else has had access, they are in the special category according to what

provided in art. 9 of the GDPR, a circumstance that implies an added risk that is

must be assessed in the risk management study and that the degree requirement increases

of protection in relation to the security and safeguarding of the integrity and

confidentiality of these data.

This risk must be taken into account by the controller who must

establish the necessary technical and organizational measures to prevent the loss of

control of the data by the person responsible for the treatment and, therefore, by the

holders of the data that provided them.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Therefore, the accredited facts constitute an infraction, attributable to the

claimed party, for violation of article 32 GDPR.

IX

Classification of the infringement of article 32 of the GDPR

The aforementioned infringement of article 32 of the GDPR supposes the commission of the infringements

typified in article 83.4 of the GDPR that under the heading "General conditions

for the imposition of administrative fines" provides:

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

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

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

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

the highest amount:

to)

the obligations of the controller and the person in charge under 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 result

appropriate to guarantee a level of security appropriate to the risk of the treatment,

in the terms required by article 32.1 of Regulation (EU) 2016/679”

X

Responsibility

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

Chapter III relating to the "Principles of the Power to sanction", in article 28

under the heading "Responsibility", the following:

"1. They may only be penalized for acts constituting an administrative offense

physical and legal persons, as well as, when a Law recognizes their capacity to

act, the affected groups, the unions and entities without legal personality and the

independent or autonomous patrimonies, which are responsible for them

title of fraud or fault."

Lack of diligence in implementing appropriate security measures

with the consequence of the breach of the principle of confidentiality constitutes the

element of guilt.

eleventh

Sanction

Article 83 "General conditions for the imposition of administrative fines" of the

GDPR in its section 7 establishes:

"Without prejudice to the corrective powers of the control authorities under the

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

can, and to what extent, impose administrative fines on authorities and bodies

public establishments established in that Member State."

Likewise, article 77 "Regime applicable to certain categories of

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 the managers or managers listed in section 1 commit

any of the offenses referred to in articles 72 to 74 of this law

organic, the data protection authority that is competent will dictate

resolution sanctioning them with a warning. The resolution will establish

likewise, the measures that should be adopted to cease the conduct or to correct it.

the effects of the offense committed.

The resolution will be notified to the person in charge or in charge of the treatment, to the body of the

that depends hierarchically, where appropriate, and to those affected who had the condition

interested, if any.

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

enough evidence for it. In this case, the procedure and the sanctions to be applied

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

be applicable.

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

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

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

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

will order the publication in the Official State or regional Gazette that

corresponds.

(…)

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.”

In this case, it is deemed appropriate to sanction the party with a warning.

claimed, for violation of article 5.1.f) of the GDPR and for violation of article 32

of the GDPR, due to the lack of diligence when implementing the appropriate measures

of security with the consequence of the breach of the principle of confidentiality.

twelfth

Measures

Article 58.2 of the GDPR provides: "Each control authority will have all the

following corrective powers indicated below:

d) order the person in charge or person in charge of the treatment that the operations of

treatment comply with the provisions of this Regulation, where appropriate,

in a specified manner and within a specified period;"

Likewise, it is appropriate to impose the corrective measure described in article 58.2.d) of the

GDPR and order the claimed party to, within a month, establish the measures

Adequate security measures so that the treatments are adapted to the requirements

contemplated in articles 5.1 f) and 32 of the GDPR, preventing them from occurring if

similar situations in the future.

The text of the resolution establishes which have been the infractions committed and

the facts that have given rise to the violation of the regulations for the protection of

data, from which it is clearly inferred what are the measures to adopt, without prejudice

that the type of procedures, mechanisms or concrete instruments for

implement them corresponds to the sanctioned party, since it is responsible for the

treatment who fully knows its organization and has to decide, based on the

proactive responsibility and risk approach, how to comply with the GDPR and the

LOPDGDD.

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:

FIRST: SANCTION the DEPARTMENT OF HEALTH OF

THE COMMUNITY OF MADRID, with NIF S7800001E, for a violation of article

5.1.f) of the GDPR, typified in article 83.5 of the GDPR.

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

SECOND: SANCTION the DEPARTMENT OF HEALTH with a WARNING

OF THE COMMUNITY OF MADRID, with NIF S7800001E, for a violation of article

32 of the GDPR, typified in article 83.4 of the GDPR.

THIRD: REQUEST the MINISTRY OF HEALTH OF THE COMMUNITY OF

MADRID, to implement, within a month, the necessary corrective measures

to adapt its actions to the personal data protection regulations, which

prevent the repetition of similar events in the future, as well as to inform this

Agency within the same term on the measures adopted.

FOURTH: NOTIFY this resolution to the MINISTRY OF HEALTH OF THE

COMMUNITY OF MADRID, with NIF S7800001E.

FIFTH: 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 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-

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

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