 Procedure No.: PS/00029/2020

938-300320

RESOLUTION OF PUNISHMENT PROCEDURE

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

based on the following

BACKGROUND

FIRST: On September 25, 2019, the director of the Agency

Spanish Data Protection Agency (hereinafter AEPD) agrees to initiate actions of

investigation in relation to a security breach of personal data (in

hereinafter Security Gap) notified by the HEALTH SERVICE OF CASTILLA-

LA MANCHA, with NIF Q4500146H, regarding the loss of data and improper access

to the history of patients in different hospitals of the aforementioned Autonomous Community.

SESCAM has notified this Agency of the following facts:

“The service of “X” of the hospital of “Y” has consulted an archived document of a

patient from the hospital itself and has been shown the documentation of a patient from the

Z's hospital. The path where the files are stored was not configured correctly

files of each patient, sharing the same location for different

hospitals. The identification of the different files was carried out by means of a

number sequence. These aspects caused the substitution of files with the

same name of different patients and the appearance of crossed documents between

different hospitals.”

They report that the security breach affects the confidentiality, integrity and

availability of basic and health data on some 431 patients.

SECOND: In view of the notified facts and the documents provided by the

responsible for the treatment, the General Subdirectorate of Data Inspection initiates

preliminary investigative actions to clarify the reported facts

by SESCAM, by virtue of its investigative powers, having knowledge of

the following extremes:

BACKGROUND

Security breach notification date: 09/16/2019

INVESTIGATED ENTITY

HEALTH SERVICE OF CASTILLA LA MANCHA (hereinafter SESCAM), with NIF

Q4500146H and with address at Avenida Río Guadiana 4, 45071 - Toledo (Toledo)

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

RESULT OF THE INVESTIGATION ACTIONS

Regarding the facts.

There has been an overlapping of attached files within the application.

□

VITROPATH tion (VITROPATH is an integrated system for managing the ser-

Anatomical Pathology service) by the users of the application in four Hospi-

such as SESCAM.

They emphasize that the improperly indexed information only corresponds to the files

ros attached to the report made by the Pathology Service. In no case is

has deindexed the report made based on the attached file, with which

that the information provided to doctors and patients is not compromised given

that the attached file is only consulted from the Pathological Anatomy Service itself.

logic.

There are 423 files that could not be recovered. It has been made known

of the Pathological Anatomy services of the affected centers to analyze

the possibility of recovering information from paper copies.

The chronology of events is as follows:

On 09/09/2019 at 12:50 a call is received at the Medical Image Support

of VITROPATH notifying that they had received an incident indicating that

from the Puertollano Hospital were consulting attached documents in VI-

TROPATH and documents from another Hospital appeared.

This incident was communicated by the Head of Service of one of the Hospitals

attached to SESCAM directly to the VITROPATH provider by email.

instead of communicating it through the IRIS incident recording system as

as it is protocolized.

The incident reaches SESCAM by telephone communication from the supplier to the group

of Medical Image Support. After analyzing the problem by the Image Support group,

Medical gene together with Middleware support it was discovered that in the deployments of

VITROPATH had not configured the path where the ad files are stored.

together, defaulting to the path c:\temp that stores the report in the directory

root of the OAS. As there is more than one VITROPATH deployment in the same OAS and

when the application uses a numerical sequence to identify the uploaded files,

documents with the same identifier have overlapped.

This incidence has caused that attached files have been overlapped and

has deindexed the patient documentation that had been attached to the

patient history in VITROPATH. Another consequence of this overlap is

that reports associated with a patient were being viewed by different Services

rent.

These attached documents correspond to requests and reports of tests carried out

zed in external centers that are attached to the VITROPATH report.

Each of the OAS where VITROPA is deployed has been analyzed.

TH to determine if other SESCAM Hospitals may have been affected.

two, verifying that the incidence has affected four hospitals attached to the

SESCAM.

Regarding the measures implemented prior to the security breach.

They have drawn up a Register of Treatment Activities (RAT), contributes

attached to this Data Inspection, with a description of the activities involved

in the gap:

"Clinical History of SESCAM" for the purpose of Management of Clinical Histories

SESCAM Patient Information

"SESCAM patients" for the purpose of data control and management

identifiers of SESCAM patients.

They do not have Risk Analysis (RA) or Impact Assessments of

For the development of the software there are controls consisting of the realization

Data Protection (EIPD).

tion of a test plan that is agreed with the company hired for this purpose.

There is an established procedure in the Area of Information Technologies

information (ATI) of SESCAM to respond, through Response Groups

to Severe Incidents (GREY), to incidents that occurred in the services of Tecno-

Information Logies.

The Severe Incident Response Groups (GRIS) are made up of, at

least one person from each of the functional units of the Department

of Operation and Service of the ATI and a person from the functional area of the Department

of ITA Projects related to the affected Information System.

Among the functions and objectives of said work team are the

take maximum care of uncertainty in the organization of the situation in the event of incidents

severe, make appropriate decisions during these processes, coordinate the action

technicians and liaise with the ATI Directorate to keep them

informed of the evolution of the event. Coordinate the necessary actions to

a fast and efficient recovery of the affected Information Systems,

so that the organization can operate normally in the shortest possible time.

ble. Prepare a report detailing the evolution of the incident from its

detection and up to the resolution, indicating the measures that should be carried out

out to avoid similar incidents in the future.

Regarding the actions and measures taken in the event of the possible occurrence of the breach.

They notify the security breach to this Agency.

On the occasion of the security breach that occurred, they provide a copy of the report

prepared by the GRIS, detailing and reporting on the evolution of the incident,

from its detection to its resolution and the measures that the Organization

has adopted to prevent and avoid similar events in the future.

As a concrete measure to prevent an incident from happening again

□

the same in the GRIS report it is indicated that "they have been included in the tests in Pro-

deployment reduction specific tasks of including attachments and reviewing

location of the file".

THIRD: On 06/24/2020, the Director of the Spanish Protection Agency

of Data agreed to initiate sanctioning proceedings against SESCAM, with NIF Q4500146H,

for the alleged infringement of articles 5.1.f) of the RGPD, in accordance with the provisions of the

article 83.5 of the RGPD and 72.1.i) of the LOPDGDD, considered very serious for the purposes of

prescription; and articles 32 and 35.3.b) of the aforementioned RGPD, in accordance with the provisions of

article 83.4 of the RGPD and article 73, sections d), e), f), g) and t) of the LOPDGDD,

considered serious for prescription purposes.

FOURTH: On 06/29/2020, the initiation agreement was notified to SESCAM, which did not

filed claims.

PROVEN FACTS

FIRST: On 09/09/2019 an incident was detected indicating that from the Hospital

of Puertollano, attached documents were being consulted in VITROPATH and

They had documents from another Hospital.

This incident was communicated directly to the VITROPATH provider by mail

electronically instead of communicating it through the IRIS incident recording system as

as it is protocolized.

SECOND: The incident has its origin in the fact that in VITROPATH deployments

the path where the attached files are stored had not been configured, being

I default to the <<c:\temp>> path that stores the report in the root directory of the OAS. To the

having more than one VITROPATH deployment in the same OAS and when using the application

tion a numerical sequence to identify the uploaded files, they have overlapped do-

documents with the same identifier.

THIRD: This incident has caused attached files to overlap and

the patient documentation that had been attached to the

patient history in VITROPATH. Another consequence of this overlap is the

access to reports associated with a patient by different Services.

FOURTH: It is verified that the incident has affected four Hospitals attached to the

SESCAM.

FOUNDATIONS OF LAW

By virtue of the powers that article 58, 64.2 and 68.1 of the RGPD recognizes to each

control authority, and according to the provisions of articles 47 and 48 of the LOPDGDD,

the director of the Spanish Agency for Data Protection is competent to initiate

and to solve this procedure.

II

The RGPD defines in article 4:

1) "personal data": any information about an identified natural person or

identifiable ("the interested party"); An identifiable natural person shall be deemed to be any person

whose identity can be determined, directly or indirectly, in particular by

an identifier, such as a name, an identification number,

location, an online identifier or one or more elements of the identity

physical, physiological, genetic, psychic, economic, cultural or social of said person;”

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

personal data or sets of personal data, whether by procedures

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

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

communication by transmission, broadcast or any other form of enabling of

access, collation or interconnection, limitation, suppression or destruction;

6) “file”: any structured set of personal data, accessible in accordance with

certain criteria, whether centralized, decentralized or distributed

functional or geographic;

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 treatment; whether the law of the Union or of the Member States

determines the purposes and means of the treatment, the person in charge of the treatment or the

Specific criteria for their appointment may be established by Union Law.

or of the Member States;

12) "personal data breach" means any breach of security

that causes 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;

15) "health-related data": personal data relating to physical or mental health

of a natural person, including the provision of health care services, which

disclose information about your health status;

According to the transcribed definitions and research carried out, it should be

conclude that the person responsible for processing the data subject to the aforementioned breach of

security is the SESCAM.

The facts notified to this Agency by SESCAM, in its capacity as responsible for the

treatment, are constitutive of infringement, attributable to SESCAM, for violation of the

article 5.1.f) of the RGPD that indicates:

<<1. The personal data will be:

f) processed in such a way as to ensure adequate security of the data

including protection against unauthorized or unlawful processing and against

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

or appropriate organizational ("integrity and confidentiality")>>.

Obligation that is modalized in article 5 of Organic Law 3/2018, of 5/12, of

Protection of Personal Data and guarantee of digital rights (hereinafter

LOPDGDD), which specifies:

<<1. Those responsible and in charge of data processing as well as all

people who intervene in any phase of this will be subject to the duty of

confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the previous section will be complementary to

the duties of professional secrecy in accordance with its applicable regulations.

3. The obligations established in the previous sections will be maintained even

when the relationship of the obligor with the person in charge or in charge of the

treatment.>>

Article 24 of the RGPD, responsibility of the data controller, provides:

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

treatment, as well as risks of varying probability and severity for

rights and freedoms of natural persons, the data controller shall apply

appropriate technical and organizational measures in order to guarantee and be able to demonstrate that

the processing is in accordance with this Regulation. These measures will be reviewed

and will update when necessary.

2. When they are provided in relation to treatment activities, between

the measures mentioned in paragraph 1 shall include the application, by the

responsible for the treatment, of the appropriate data protection policies>>.

Article 25 of the RGPD establishes the obligations indicated below:

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

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

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

natural persons, the data controller will apply, both at the time of

determine the means of treatment as at the time of the treatment itself,

appropriate technical and organizational measures, such as pseudonymisation, designed

to effectively apply the principles of data protection, such as the

minimization of data, and integrate the necessary guarantees in the treatment, in order to

comply with the requirements of this Regulation and protect the rights of

interested.

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

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

the personal data that is necessary for each of the specific purposes of the

treatment. This obligation will apply to the amount of personal data collected, to

the extension of its treatment, its conservation period and its accessibility. Such

measures shall in particular ensure that, by default, personal data is not

accessible, without the intervention of the person, to an indeterminate number of people

physical.>>

Article 28.1 and 2 of the LOPDGDD, regarding the general obligations of the

responsible and in charge of the treatment, indicates the following:

<<1. Those responsible and in charge, taking into account the elements listed in

Articles 24 and 25 of Regulation (EU) 2016/679, will determine the technical measures

and appropriate organizational measures that must be applied in order to guarantee and certify that the

treatment is in accordance with the aforementioned regulation, with this organic law, its

implementing regulations and applicable sectoral legislation. In particular, they will assess whether

proceeds to carry out the impact assessment on data protection and the

prior consultation referred to in Section 3 of Chapter IV of the aforementioned regulation.

2. For the adoption of the measures referred to in the previous section, the

controllers and processors shall take into account, in particular, the

greater risks that could occur in the following cases:

a) When the treatment could generate situations of discrimination, usurpation of

identity or fraud, financial loss, reputational damage, loss of

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

pseudonymization or any other significant economic, moral or social damage to

the affected.

b) When the treatment could deprive those affected of their rights and freedoms or

could prevent them from exercising control over your personal data.

c) When the non-merely incidental or accessory treatment of the

special categories of data referred to in articles 9 and 10 of the Regulation

(EU) 2016/679 and 9 and 10 of this organic law or data related to the commission

of administrative offenses.

f) When there is massive processing involving a large number of

affected or involves the collection of a large amount of personal data.>>

Article 35.1 and 35.3.b) of the RGPD, on the impact assessment related to the

data protection, indicate the following:

<<1. When a type of treatment, particularly if it uses newer

technologies, due to their nature, scope, context or purposes, entails a high risk for

rights and freedoms of natural persons, the data controller will perform,

prior to treatment, an assessment of the impact of treatment operations on

the protection of personal data. A single assessment may address a number of

similar processing operations involving similar high risks>>.

<<3. The impact assessment relating to data protection referred to in the

paragraph 1 will be required in particular in case of:

b) large-scale treatment of the special categories of data referred to in the

article 9, paragraph 1, or personal data relating to convictions and offenses

penalties referred to in article 10>>.

In accordance with the provisions of article 35.4 of the RGPD, the AEPD has established and published a

list of types of processing operations that require an evaluation of

impact.

This list is based on the criteria established by the Article 29 Working Group in

the guide WP248 “Guidelines on impact assessment related to the protection of

data (EIPD) and to determine if the treatment is "likely to carry a high risk"

for the purposes of the RGPD”, complements them and should be understood as a non-exhaustive list:

(…)

<<4. Treatments that imply the use of special categories of data to which

refers to article 9.1 of the RGPD, data related to convictions or criminal offenses to the

referred to in article 10 of the RGPD or data that allow determining the situation

financial or asset solvency or deduce information about people

related to special categories of data>>.

In the aforementioned document (WP248, page 15, III.c) it states the following:

<<The requirement to carry out an DPIA applies to existing processing operations

which are likely to pose a high risk to the rights and freedoms of

natural persons and for whom there has been a change in risks, taking into account

account the nature, scope, context and purposes of the treatment.

An EIPD will not be necessary for treatment operations that have been verified

carried out by a control authority or the data protection delegate, in accordance with

ity with article 20 of Directive 95/46/EC, and that they are carried out in a way that does not

has changed since the previous check. In fact, “[t]he decisions of the Co-

mission and authorizations of the control authorities based on the Directive

95/46/EC remain in force until they are modified, replaced or repealed»

(recital 171).

Instead, this means that treatments whose

application conditions (scope, purpose, personal data collected, identity of the

data controllers or recipients, data retention period, measures

technical or organizational measures, etc.) have changed since the previous check

carried out by the control authority or the data protection delegate and that proves

probably entail a high risk.

In addition, an DPIA may be required after a change in the

risks due to treatment operations, for example due to the commissioning of

development of a new technology or that personal data is used for a different purpose.

red. Data processing operations can evolve rapidly and can

new vulnerabilities emerge. Therefore, it should be noted that the revision of a

DPIA is not only useful for continuous improvement, it is also essential

to maintain the level of data protection in an environment that evolves with the

weather. An DPIA may also become necessary due to changes in the context

organizational or social nature of the processing activity, for example because the effects

certain automated decisions have gained importance or that

new categories of stakeholders become vulnerable to discrimination. Each

one of these examples could be an element that causes a change in the relative risk

resulting from the treatment activity in question.

In terms of context, the data collected, purposes, functionalities, personal data
treated, recipients, data combinations, risks (means of support, causes of
risk, possible effects, threats, etc.), security measures and international transfers.
nationals.

Instead, certain changes could also reduce the risk. For example, an operation
treatment could evolve so that decisions were no longer auto-
nuanced or an observation activity was no longer systematic. In that case, the
view of the risk analysis performed may show that the performance is no longer required.
tion of a DPIA.

For reasons of good practice, an EIPD must be continuously reviewed and re-evaluated.
luada regularly. Therefore, even if on May 25, 2018, a
EIPD, it will be necessary, at the appropriate time, for the data controller to reach
sees such an assessment carried out as part of its general duties of
proactive responsibility.>>.

Consequently, an EIPD must be carried out if it is not available or, in its
case, review the existing one and reevaluate it after the new modifications of the treatments.
Data collected within the scope of the VITROPATH application.

III

Article 83.5 a) of the RGPD, considers that the infringement of <<the basic principles
for treatment, including the conditions for consent under the articles
articles 5, 6, 7 and 9" is punishable, in accordance with section 5 of the aforementioned article
83 of the aforementioned Regulation, with administrative fines of a maximum of €20,000,000 or,
in the case of a company, an amount equivalent to a maximum of 4% of the volume
overall annual total turnover of the previous financial year, opting for the
higher amount.>>

Article 83.4 a) of the RGPD, indicates: <<Infractions of the following provisions

will be sanctioned, in accordance with section 2, with administrative fines of 10,000

EUR 000 maximum or, in the case of a company, an amount equivalent to 2

Maximum % of the total global annual turnover of the previous financial year

higher, opting for the highest amount: a) the obligations of the controller and the processor

under articles 8, 11, 25 to 39, 42 and 43>>.

Article 83.7 of the RGPD indicates:

IV

<<Without prejudice to the corrective powers of the control authorities under art.

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

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

established in that Member State>>

Article 58.2. b) and d) of the RGPD indicates the following:

<<Each control authority will have all the following corrective powers

listed below:

b) sanction any person responsible or in charge of the treatment with a warning

when the treatment operations have violated the provisions of this Regulation.

glament;

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

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

in a certain way and within a specified period>>.

For its part, the Spanish legal system has chosen not to sanction with a fine

public entities, as indicated in article 77.1. c) and 2. 4. 5. and 6 of the

LOPDDGG:

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

who are responsible or in charge:

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

autonomous and the entities that make up the Local Administration.

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

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

organic, the data protection authority that is competent will issue a resolution

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

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

offense that had been 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 party, if any.

4. The data protection authority must be notified of the resolutions that

fall in relation to the measures and actions referred to in the sections

previous.

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.

6. When the competent authority is the Spanish Data Protection Agency,

this will publish on its website with due separation the resolutions referring to

the entities of section 1 of this article, with express indication of the identity of the

responsible or in charge of the treatment that had committed the infraction.>>

v

In the present case, from the investigations carried out by this Agency,

It follows that SESCAM has violated the principle of confidentiality by allowing

improperly access to the health data of 431 patients by personnel not

authorized. Likewise, it has violated the principle of integrity by not guaranteeing the

security of the health data of 431 patients against loss, destruction or damage

by applying appropriate technical or organizational measures.

There is also no evidence that SESCAM has carried out the appropriate risk analysis and

mandatory impact assessment in accordance with the provisions of article 35 of the

GDPR.

Therefore, in accordance with the applicable legislation and having assessed the criteria for

graduation of the sanctions whose existence has been proven, the Director of the

Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE CASTILLA LA MANCHA HEALTH SERVICE, with NIF

Q4500146H, for the infringement of article 5.1.f) of the RGPD, in accordance with the provisions of the

article 83.5 of the RGPD and 72.1.i) of the LOPDGDD, considered very serious for the purposes of

prescription, a sanction of warning; and articles 32 and 35.3.b) of the aforementioned

RGPD, in accordance with the provisions of article 83.4 of the RGPD and article 73, sections d),

e), f) and g) of the LOPDGDD, considered serious for prescription purposes, a sanction

of warning.

SECOND: TO REQUEST the CASTILLA LA MANCHA HEALTH SERVICE to

contribution within six months:

 Risk analysis and impact assessment of treatment operations

of personal data within the scope of the VITROPATH application as

provided in article 35 of the RGPD.

 Audit after the notified security breach that certifies that the

personal data processing operations within the scope of the application

VITROPATH are in accordance with the provisions of the RGPD.

THIRD: NOTIFY this resolution to the CASTILLA HEALTH SERVICE

LA MANCHA, with NIF Q4500146H and with address at Avenida Río Guadiana 4,

45071 Toledo.

FOURTH: COMMUNICATE this resolution to the Ombudsman,

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

FIFTH: COMMUNICATE this resolution to the DEPARTMENT OF HEALTH OF

CASTILLA LA MANCHA, with NIF S1911001D, Plaza Conde 2, 45002, Toledo.

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

LPACAP, the interested parties may optionally file an appeal for reconsideration

before the Director of the Spanish Agency for Data Protection within a period of

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

contentious-administrative appeal before the Contentious-Administrative Chamber of the

National Court, in accordance with the provisions of article 25 and section 5 of

the fourth additional provision of Law 29/1998, of July 13, regulating the

Contentious-administrative jurisdiction, within a period of two months from the

day following the notification of this act, as provided in article 46.1 of the

aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the

LPACAP, the firm resolution may be provisionally suspended in administrative proceedings

through the

if the interested party expresses his intention to file a contentious appeal-

administrative. If this is the case, the interested party must formally communicate this

made by writing to the Spanish Agency for Data Protection,

introducing him to

the agency

[https://sedeagpd.gob.es/sede-electronica-web/], or through any of the other

records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. Also

must transfer to the Agency the documentation that proves the effective filing

of the contentious-administrative appeal. If the Agency were not aware of the

filing of the contentious-administrative appeal within two months from the

day following the notification of this resolution, it would end the

precautionary suspension.

Electronic Registration of

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es