 File No.: PS/00268/2022

RESOLUTION OF SANCTIONING PROCEDURE

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

to the following

BACKGROUND

FIRST: ASSOCIATION OF CONSUMERS AND USERS IN ACTION OF

MADRID FACUA, (hereinafter, FACUA), on June 14, 2021 filed

claim before the Spanish Data Protection Agency. The claim is

directed against HEALTH MINISTRY OF THE COMMUNITY OF MADRID, with NIF

S7800001E, (hereinafter CONSEJERY). The reasons on which the claim is based are

the following:

-That, due to a programming error, data from

personal character (ID card, telephone number, date of birth and phone numbers)

health identification) of citizens when accessing the self-appointment website, activated by

the Community of Madrid on May 24. This platform of the Community of Madrid

has been created so that citizens who had not yet received any dose of

the COVID-19 vaccine could schedule an appointment for their vaccination, according to

has been able to verify the digital communication medium EL DIARIO.ES.

Together with the claim, a screenshot of the home page of the application is provided.

COVID self-citation from the Health Department of the Autonomous Community of Madrid, and

the news published by elDiaro.es on 06/15/2021, which includes a screenshot of the

data that appear in said application, although in the attachment as an example they have been

Anonymized all except the name “A.A.A.”.

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

December, Protection of Personal Data and guarantee of digital rights (in

hereafter LOPDGDD), the claim presented by FACUA was forwarded to the

CONSEJERIA, to proceed with its analysis and inform this Agency in the

period of one month, of the actions carried out to adapt to the requirements

provided for in the data protection regulations.

The transfer, which was carried out in accordance with the regulations established in Law 39/2015, of

October 1, of the Common Administrative Procedure of the Administrations

Public (hereinafter, LPACAP), was collected on 06/18/2021 as stated in the

acknowledgment of receipt in the file.

No response has been received to this letter of transfer.

THIRD: On September 10, 2021, in accordance with article 65 of

the LOPDGDD, the claim presented by FACUA was admitted for processing.

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 functions assigned to the control authorities in the

article 57.1 and the powers granted in article 58.1 of the Regulation (EU)

2016/679 (General Data Protection Regulation, hereinafter GDPR), and

in accordance with the provisions of Title VII, Chapter I, Second Section, of the

LOPDGDD, having knowledge of the following extremes:

INVESTIGATED ENTITY

During these proceedings, the following entity has been investigated:

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

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

(MADRID)

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

RESULT OF INVESTIGATION ACTIONS

1.- On June 10, 2021, the digital media ElDiario.es published an article in

which was informed, among others, of the following:

“The Community of Madrid activated its self-appointment system on May 24

by age ranges so that citizens who had not yet received

no dose of the COVID-19 vaccine could schedule an appointment.

From that day until this Thursday, the website set up by the Ministry

of Health to request that summons has had a security breach that has

affected all people with a health card in the region, according to

able to verify elDiario.es.

Due to a programming error, the page left the name

complete, ID, telephone number, date of birth and the numbers of

health identification both regional and national of any

citizen when an appointment request was made with their CIPA number (Code

of Personal Identification of the Community of Madrid).

Said article also publishes what it argues are the data of a citizen

Affected by the security breach of the "autocita" portal to get vaccinated against

coronavirus of the Community of Madrid, in which it can be seen that in the web code

The data corresponding to the following fields are crossed out: NIF, name,

lastname1, lastname2, date of birth, phone number, gender, and phone numbers

health identification, both regional and national.

In the image published by the media, it can be seen that in the tab

“red”, within the browser inspection tool, a JSON (network notation)

JavaScript object, is a simple text format for data exchange) in the

that the aforementioned data appears with the content hidden

willfully.

The article also mentions that this information was not visible to the naked eye, but rather

was present in the computer code of the Web and that to access it you had to

turn on browser developer tools, an option that is

available to any user but not usually used without certain knowledge

previous technicians.

It also informs that the gap has been closed after receiving a notice from

of the media.

2.- On October 5, 2021, a data inspection request was made to the

DEPARTMENT OF HEALTH OF THE COMMUNITY OF MADRID, hereinafter the

Counseling, the following documentation and information:

1. Detailed and chronological description of the events that occurred.

2. Detailed specification of the causes that have made the incident possible.

3. Number of people affected by the data security breach

personal.

4. Category of personal data involved.

5. Possible consequences for the people affected.

6. Detailed description of the actions taken to resolve the incident and

minimize its impact on affected people.

7. Security measures for the processing of personal data adopted with

prior to the incident, as well as supporting documentation of the Analysis

of Risks that the implementation of said security measures has entailed

and, where appropriate, a copy of the Impact Evaluations of the treatments where

there has been a breach of personal data security.

8. Copy of the Activity Record of the treatments where the error occurred.

incident.

9. If the security breach has been notified to the affected persons, indicate

the channel used, date of communication and details of the message sent.

If not, indicate the reasons.

10. Reason why the breach has not been reported within 72 hours of

happen.

11. Any other that you consider relevant.

Said requirement was notified through the Electronic Address service

Unique Enabled and was accepted by the recipient on October 10, 2021, according to

accredit said service.

On October 21, 2021, a letter was received from the Delegate Committee for the Protection of

Data from the Ministry requesting an extension of the term to respond to the

application.

3.- After the period given to respond to the request for information without obtaining

response, dated December 1, 2021, the request for information was reiterated to the

Counseling, through the Unique Authorized Electronic Address service and was

accepted by the addressee on December 2, 2021, as evidenced by said

service.

4.- Given the lack of response to the data inspection requirements, dated

March 14, 2022 the Director of the Spanish Data Protection Agency

agrees to start a disciplinary procedure against the Ministry, for the infringement of the

Article 58.1 of the General Data Protection Regulation (RGPD), typified in the

art. 83. 5 e) of the aforementioned GDPR, within the framework of which, the defendant body alleges that

the Delegate Committee for Data Protection of the Department, in the exercise of its

functions, sent a response to the request for data inspection through

document dated February 1, 2022 with reference to the Presentation Record

REGAGE22e00002434053 and provide supporting documentation for presentation in the

record and copy of the letter of attention to the information requirement, in which

reveal the following:

Regarding the causes that have made the incident possible:

-

After analyzing the facts, they conclude that the failure detected related to this

information system is due to an exposure of data information

personal (public) accessed using a valid session cookie, and editing

the URL accessed one of the input fields called "idPaciente" with an ID

valid. In this way, a series of personal data can be displayed

corresponding to the person with the ID used. Additionally, it is found that

the web application had insufficient blocking mechanisms against

retries when entering the authentication data (Authentication Code)

Autonomous Population Identification [CIPA], Date of birth and DNI) for

request the appointment.

Regarding the affected data

- There is no record in the Ministry of Health that the failure occurred
affected no citizen, beyond the information published in the media
Communication. Likewise, there is no record of any
any damage to the freedoms and rights of citizens.
- Only identifying data of the users could have been affected.
citizens: Name and Surname, CIPA, Date of birth, patient ID, DNI,
Telephone number, Sex.
- There is no record in the Ministry of Health that there has been a
damage to the freedoms and rights of citizens, without having verified
up to the date that has resulted in material or non-material damage in the
citizens who may have been affected. The correction of this
vulnerability was prior to its dissemination in the media.

Detailed description of the actions taken to resolve the incident and minimize
its impact on the people affected:

- The application was modified in order to improve the
information system and the version was uploaded, being the following
the most relative changes:

June 9:

Minimize the information to be exchanged between the user's browser and
the server. Only information that is displayed on the screen or that the
user has previously entered. No number is exchanged in any case.

telephone, CIP SNS (Population Identification Code of the National System of

Health), sex. The rest (date of birth, name and surname) are shown by

screen.

 Request the verification code sent by SMS as the first step, nothing more

enter the identification data.

 Do not return specific error codes, only generic ones.

The data required in the identification process is increased, offering two

possibilities to the user:

or CIPA + Date of birth + DNI

o DNI/NIE/PASSPORT + Date of birth + First surname

- The design of the architecture of the application does not allow the modification of the data

user affiliation. Because the application makes use of a database

independent and the requested mobile is only used as part of the OTP

implemented to validate the appointment request.

Regarding security measures

- The SERMAS development team uses a development methodology

continuously updated collected in (...) in the Ministry of Health of the

Madrid's community.

They provide a copy of (...), whose objective is to have the standards that must be

fulfill the applications from the technical and functional point of view, as well as the

whitepapers describing the platforms they should integrate with

the same. The indications and guidelines (...) are mandatory for

all the developments of new applications for the DGSIS.

- The point (...) establishes regarding the access to the applications of the citizens the

following:

(…)

- They state in relation to the impact assessment (EIPD) on the present

treatment, taking into account its nature, scope, context and purposes, as well as

that in the present treatment there is no systematic evaluation and

exhaustive analysis of personal aspects that is based on automated processing,

nor is there a treatment of special categories of data. Therefore, it

considers that in the present treatment it is not necessary to carry out a

EIPD.

5.- It has been verified by the inspection of data that in the Internet Archive (library

digital managed by a non-profit organization containing millions of

Internet pages recorded since 1996) has registered the web page

https://autocitavacuna.sanidadmadrid.org existing on the date of June 14, 2021,

in which it can be verified that to request an appointment for the vaccine

only the CIPA code and if you do not have said code, ID and

birthdate.

CONCLUSIONS

- Regarding the causes that have made possible the incident published in

ElDiario.es, the representative of the Ministry states that, after analyzing the facts conclude that the fault detected related to this system of information is due to an exposure of personal data information (public) accessed using a valid session cookie, and editing the URL accessed one of the entry fields called "idPaciente" with a valid ID.

This explanation does not agree with the security incident communicated to this Agency by FACUA, incident for which personal data was exposed when making an appointment request with a CIPA number (Code of Personal Identification of the Community of Madrid) existing. It has been proven by the inspection of data that Internet Archive keeps the web page https://autocitavacuna.sanidadmadrid.org existing on the date of June 14, 2021, in which it can be verified that to request an appointment for the vaccine it only requests the CIPA code and if it does not have said code, it will request ID and date of birth.

On the other hand, the representative of the Ministry acknowledges that, among the actions taken to solve the incident, information has been reduced to a minimum to exchange between the user's browser and the server. is only transmitted information that is displayed on the screen or that the user has entered previously. No telephone number, CIP SNS is exchanged in any case (National Health System Population Identification Code), sex. He The rest (date of birth, name and surname) are shown on the screen. Besides, The data required in the identification process has been increased, offering two possibilities to the user: CIPA + Date of birth + DNI or DNI/NIE/PASSPORT + Date of birth + First surname.

- Regarding security measures, the Madrid Health Service (SERMAS) dependent on the Department, it uses a methodology of development of

computer applications that are collected in (...) of the Community of Madrid.

o The (...) relative to authentication establishes regarding access to the

Citizen applications the following:

(…)

It has been verified by data inspection that Internet Archive

retains the existing web page https://autocitavacuna.sanidadmadrid.org

on the date of June 14, 2021, in which it can be verified that for

request an appointment for the vaccine, only the CIPA code is requested and, if

If you do not have said code, ID and date of birth are requested.

o The (...) named (...) establishes, among others, the following:

(…)

It is unknown if the Ministry has carried out a risk analysis,

as established by the methodology (…).

o It (...) establishes the following:

(…)

It is unknown if the tests and analyzes have been carried out

of this treatment by the Security Office, according to

establishes the methodology (…).

FIFTH: On July 15, 2022, the Director of the Spanish Agency for

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

for the alleged infringement of Article 5.1.f) of the GDPR, Article 33 of the GDPR, Article

25 of the GDPR and Article 32 of the GDPR, typified in Article 83.5 of the GDPR.

Once the Initiation Agreement was notified, the MINISTRY presented a written statement of allegations in the

which in summary stated:

-That in the months of May and June 2021, we were at a very

critical related to the management of the pandemic. In this period, in which the

vaccination process to the population in general -although in a staggered manner by

age ranges-, urgently required the organization and opening of said

process in a massive way and, consequently, it was necessary to offer a

system with clear and simple information on the process to be followed by the

citizenship and the urgency required for its adoption at the organizational level, including

also several channels to facilitate the summons of the citizenship.

This state of health emergency made it necessary to develop a

large number of new tools with great speed to be able to provide the best

service to citizens through the development and deployment of the summons process

for vaccination in an agile way in authorized centers, even allowing the

citizen to select the time and center of their preference, which made it easier for the

Comunidad de Madrid reached a high number of vaccinated population,

contributing with said action to be able to face this situation of

pandemic as soon as possible, and facilitate the mobility of the population before the start of

periods traditionally considered as holidays in which there would be

the mobility of the population.

-In this regard, this Agency recalls that both article 25.1 of the GDPR

such as 32 of the same legal text, emphasize the need that, both in the

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

own treatment, the person in charge adopts technical and organizational measures

appropriate to effectively apply the data protection principles

and guarantee a level of security appropriate to the risk, without being able to accept

as exempted by the circumstance of haste alleged by health emergency.

It is not possible to appreciate, in the present case, a state of necessity that justifies the

production of a defective application, which allowed access to

personal data of a large number of citizens, without carrying out

previously the necessary verifications to determine its correct

functioning, and whose use can cause a greater evil than that which is

intends to avoid.

-That in the initiation agreement reference is made in the section "Regarding the

security measures" to the point (...), which is generic, and which for Autocita is

enabled other access procedures so that citizens who do not

who had a Health Card of the Community of Madrid, could request the

vaccination through the website. Therefore, they consider that the reference (...)

It should be deleted as it is not related to this specific case.

-In this regard, this Agency has simply reflected the information

provided by the DEPARTMENT itself in its response to the request for

information carried out by the AEPD, in which they attach a (...) to which they make

Reference in paragraph 6 of your answer:

“6. Security measures for personal data processing adopted

prior to the incident, as well as supporting documentation of the

Risk Analysis that the implementation of said security measures has entailed

security and, where appropriate, a copy of the Impact Assessments of the

Treatments where the data security breach has occurred

personal".

And that, according to the CONSEJERIA itself, is the development methodology

used.

-That measures have been established for the continuous improvement of crisis management and

cyber incidents, focused on the prevention, detection and response to incidents of

security. Specifically, the following measures have been implemented to

strengthen security:

• The development and production process of applications has been reviewed, such as

part of the process of continuous improvement in the cycle of development and start-up of

applications, placing special emphasis on the following aspects:

o Reinforcement of the resources allocated to the prior validation of the security of the

application before it goes into production.

o Reinforcement of penetration testing and analysis methods

code to all self-developed systems and will not be put into production

even solving the possible vulnerabilities detected.

o Reassessment of all self-developed systems to verify that they

High or Critical vulnerabilities have been corrected,

detected during the "pentest" phase.

• The (...) has been revised, updating the main areas to take into account when

of developing applications, as well as the main tasks tasks to take into account

when implementing applications in the Continuous Integration structure and

Continuous Deployment in the CSCM, in order to have the most

standards that applications must comply with from a technical point of view and

functional, as well as the technical documents that describe the platforms with which

which must be integrated.

• The use cases in security audits have been improved.

Lastly, it is relevant to mention that work is currently being done on a

project to adopt a tool (...).

-In this regard, this Agency values positively the adoption of new

measures that result in greater security in terms of the treatment of

personal data is concerned and that can prevent, in the future, incidents

as the one that is substantiated in the present proceeding.

-That the (...) is part of the security regulatory body of the CSCM and is

is classified as a RESTRICTED USE document, therefore it is

considered a controlled dissemination document and its use is restricted to personal

internal to the organization, since its public dissemination may pose a risk

for security. The content (...) constitutes confidential information whose dissemination,

outside the organization or the scope of people who do not need to know said

information, can cause harm or cyber attacks on the

Services considered essential by law.

Therefore, it is required that such information, given its extraordinary sensitivity, be

reservation object and consequently no content information is displayed

(...) in the Resolution that falls under this procedure and that could, in its

case, be published.

-In this regard, this Agency states that the documentation in the

file is used exclusively to carry out an exhaustive and correct

instruction of the same, not being, in any case, of public access. Even

in the event that in the decision handed down there is some kind of

information of restricted use, it would proceed to its anonymization as a step

prior to its publication.

SIXTH: On August 12, 2022, a resolution proposal was formulated,

proposing that the Director of the Spanish Data Protection Agency

sanction the MINISTRY OF HEALTH, with NIF S7800001E,

-For an infringement of Article 5.1.f) of the GDPR, typified in article 83.5 of the

GDPR, with a warning.

-For a violation of Article 25 of the GDPR, typified in article 83.4 of the GDPR,

with a warning.

-For a violation of Article 32 of the GDPR, typified in article 83.4 of the GDPR,

with a warning.

-For a violation of Article 33 of the GDPR, typified in article 83.4 of the GDPR,

with a warning.

SEVENTH: Once the proposed resolution has been notified, the DEPARTMENT presents a new

pleadings in which, in summary, reproduces those already submitted to the Agreement

Start, and adds that:

– Notification to the AEPD. As indicated in the first letter sent to the AEPD

in relation to this disciplinary procedure, depending on the level of risk of the

incidence, taking into account the low volume of data that could have been

affected, the type of the same, being only character data

identification, and the non-existent impact caused to the interested parties, it was estimated that it was mandatory to inform the Control Authority.

Thus, article 33 of the GDPR states that "In the event of a breach of the security of personal data, the person responsible for the treatment will notify it to the authority of competent control in accordance with article 55 without undue delay and, if necessary possible, no later than 72 hours after it has become aware of it, to unless it is unlikely that such a security breach would constitute a risk for the rights and freedoms of natural persons".

Therefore, in the present case, as we have indicated, taking into account that neither At that time, or currently, there is evidence that no citizen has suffered negative consequences in their rights and freedoms, taking into account consideration additionally that a significant number have not been affected of personal data, nor have special category data of the citizens, it was considered at the time that said communication was not necessary since it was unlikely to constitute a risk to the rights and liberated from citizens.

– Security measures taken initially. In addition to the above, as indicated In the initial communication to the AEPD, from the design the tool had adequate security measures to avoid, both that the impact of possible security incidents were high, such as the same happening.

Thus, in the first letter sent it was already indicated that at all times the channel of Communication between the user and the SERMAS servers are secured. He Application architecture design does not allow modification of application data. user affiliation. Because the application makes use of a database

independent and the requested mobile is only used as part of the OTP (One

Time Password) implemented to validate the appointment request.

In the same way and to correct what happened, once the failure was known and

identified it, before it was published in the media,

The application was modified in order to improve the

information system and the version was uploaded, being the following

the most relative changes:

June 9:

(…)

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: It is proven that on 05/24/2021, the MINISTRY activated a

self-appointment system so that citizens could request an appointment to get vaccinated

against COVID-19.

SECOND: It is proven that there was a failure in the system, due to which

personal (public) data was exposed by accessing through a cookie

valid session, and editing the URL accessed in one of the input fields called

"idPaciente" with a valid ID.

THIRD: It is proven that the web application had mechanisms of

Insufficient blocking before retries when entering the authentication data.

FOURTH: It is proven that, after being aware of the security breach,

the MINISTRY did not communicate it to the AEPD.

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 relation to the allegations presented to the resolution proposal, the

CONSEJERIA reiterates those already presented previously and adds that:

II

1-Regarding the notification of the breach to the AEPD, depending on the level of risk

of the incident, taking into account the low volume of data that could have been

affected, the type of the same, being only character data

identification, and the non-existent impact caused to the interested parties, it was estimated that

it was mandatory to inform the Control Authority.

In the present case, taking into account that, neither at that time nor currently,

there is evidence that no citizen has suffered negative consequences in

their rights and freedoms, additionally taking into consideration that they have not been

A significant number of personal data have been affected, nor have they been affected

special category data of citizens, it was estimated at the time that said

communication was not necessary since it was unlikely that a

risk to the rights and freedoms of citizens.

-In this regard, this Agency indicates that it has not been submitted by the

CONSEJERIA a risk assessment actually carried out, resulting, for

therefore, very indeterminate the concept of: "it was improbable that the

a risk to the rights and freedoms of citizens”

2- Security measures taken initially. In addition to the above, as indicated

In the initial communication to the AEPD, from the design the tool had

adequate security measures to avoid, both that the impact of possible

security incidents were high, such as the same happening.

-In this regard, this Agency confirms that, in fact, the incidents do

materialized, that a failure was detected in the system, due to a

exposure of personal (public) data information accessed through

a valid session cookie, and by editing the URL accessed one of the fields of

entry called "idPaciente" with a valid ID.

Additionally, it was verified that the web application had mechanisms of

Insufficient blocking before retries when entering the data of

authentication.

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

II

"1. Personal data will be:

(…)

f) processed in such a way as to guarantee adequate 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 the present case, it is clear that the personal data of those affected, held in the

CONSEJERIA database, were improperly exposed to a third party,

according to the news published in elDiario.es.

From the instruction carried out in this proceeding it is concluded that the

CONSEJERIA has violated the provisions of article 5.1.f of the GDPR.

The infringement is typified in article 83.5 of the RGPD that under the heading "Conditions

rules for the imposition of administrative fines" provides:

IV.

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

paragraph 2, with administrative fines of maximum EUR 20,000,000 or,

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

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

the highest amount:

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

consent under articles 5, 6, 7 and 9; (…)”

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that:

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result

contrary to this organic law”.

For the purposes of the limitation period, article 72 "Infractions considered very

serious" of the LOPDGDD indicates:

"1. Based on what is established in article 83.5 of Regulation (EU) 2016/679,

are considered very serious and will prescribe after three years the infractions that

a substantial violation of the articles mentioned therein and, in particular, the

following:

a) The processing of personal data in violation of the principles and guarantees

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

Without prejudice to the provisions of article 83.5 of the GDPR, the aforementioned article provides in

its section 7 the following:

V

"7. 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.

For its part, 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

autonomous communities 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.

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. (…)”

Article 25.1 of the GDPR indicates:

SAW

"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 severity involved in the treatment 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 data protection principles, 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.”

In the present case, it is clear that a failure has been detected in the system, due to a

exposure of personal (public) data information accessed through a

valid session cookie, and editing the URL accessed one of the input fields

called "idPaciente" with a valid ID. Additionally, it is detected that the application

website had insufficient blocking mechanisms against retries at the time of

Enter the authentication data.

From the instruction carried out in this proceeding it is concluded that the

CONSEJERIA has violated the provisions of article 25.1 of the GDPR,

The infringement is typified in article 83.4 of the RGPD that under the heading "Conditions

rules for the imposition of administrative fines" provides:

VII

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

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

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

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

the highest amount:

a) the obligations of the person in charge and the person in charge according to articles 8,

11, 25 to 39, 42 and 43; (…)”

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result

contrary to this organic law”.

For the purposes of the limitation period, article 73 "Infractions considered serious"

of the LOPDGDD indicates:

"Based on what is established in article 83.4 of Regulation (EU) 2016/679,

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

substantial violation of the articles mentioned therein and, in particular, the

following:

(…)

d) The lack of adoption of those technical and organizational measures that

are appropriate to effectively apply the principles of protection

of data from the design, as well as the non-integration of the guarantees

necessary in the treatment, in the terms required by article 25 of the

Regulation (EU) 2016/679. (…)

Without prejudice to the provisions of article 83.5 of the GDPR, the aforementioned article provides in its section 7 the following:

VIII

“7. 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.

For its part, 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 autonomous communities 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.

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. (…)”

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

IX

"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

technical and organizational measures to guarantee the safety of the

treatment.

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

take into account the risks presented by data processing, in particular as

consequence of the destruction, loss or accidental or illegal alteration of data

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

unauthorized access to such data.

3. Adherence to an approved code of conduct pursuant to article 40 or to a

certification mechanism approved under article 42 may serve as an element

to demonstrate compliance with the requirements established in section 1 of the

present article.

4. The controller and the processor shall take measures to ensure that

any person acting under the authority of the controller or processor and

have access to personal data can only process such data by following

instructions of the person in charge, unless it is obliged to do so by virtue of the Law of

the Union or of the Member States.

In the present case, at the time of the breach, the DEPARTMENT did not

had the appropriate technical and organizational measures in place to prevent

produced an incident such as the one at issue in this proceeding, since

once the CIPA code was entered, a second authentication was not required, nor were the

personal data appeared pseudonymised.

From the instruction carried out in this proceeding it is concluded that the

CONSEJERIA has violated the provisions of article 32 of the GDPR,

The infringement is typified in article 83.4 of the RGPD that under the heading "Conditions

rules for the imposition of administrative fines" provides:

x

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

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

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

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

the highest amount:

a) the obligations of the person in charge and the person in charge according to articles 8,

11, 25 to 39, 42 and 43; (…)”

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result

contrary to this organic law”.

For the purposes of the limitation period, article 73 "Infractions considered serious"

of the LOPDGDD indicates:

"Based on what is established in article 83.4 of Regulation (EU) 2016/679,

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

substantial violation of the articles mentioned therein and, in particular, the

following:

(…)

f) The lack of adoption of those technical and organizational measures that

are appropriate to guarantee a level of security appropriate to the risk

of the treatment, in the terms required by article 32.1 of the Regulation

(EU) 2016/679.

(…)

Without prejudice to the provisions of article 83.5 of the GDPR, the aforementioned article provides in

its section 7 the following:

eleventh

“7. 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.

For its part, 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

autonomous communities 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.

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. (…)”

Article 33 "Notification of a violation of the security of personal data to

the control authority” of the GDPR establishes:

twelfth

"1. In the event of a breach of the security of personal data, the person responsible for the

treatment will notify the competent control authority in accordance with the

Article 55 without undue delay and, if possible, no later than 72 hours after

that he became aware of it, unless it is unlikely that said violation

of security constitutes a risk to the rights and freedoms of individuals

physical. If the notification to the control authority does not take place within the period of 72

hours, must be accompanied by an indication of the reasons for the delay.

2. The person in charge of the treatment will notify without undue delay the person in charge of the

treatment of violations of the security of personal data of which it has

knowledge.

3. The notification referred to in section 1 must, at least:

a) describe the nature of the data security breach

including, where possible, the categories and number

number of affected stakeholders, and the categories and approximate number

of affected personal data records;

b) communicate the name and contact details of the data protection delegate

data or other contact point where more information can be obtained;

c) describe the possible consequences of the breach of the security of the

personal information;

d) describe the measures adopted or proposed by the person responsible for the

processing to remedy the data security breach

personal information, including, if applicable, the measures taken to mitigate the

possible negative effects.

4. If it is not possible to provide the information simultaneously, and to the extent that

is not, the information will be provided gradually without undue delay.

5. The controller will document any breach of the security of

personal data, including the facts related to it, its effects and the

corrective measures taken. Said documentation will allow the authority of

control to verify compliance with the provisions of this article."

In the present case, it is clear that the MINISTRY has suffered a security breach

of personal data on 05/24/2021 and has not informed this Agency.

From the instruction carried out in this proceeding it is concluded that the

CONSEJERIA has violated the provisions of article 33 of the GDPR.

The infringement is typified in article 83.4 of the RGPD that under the heading "Conditions

rules for the imposition of administrative fines" provides:

XIII

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

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

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

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

the highest amount:

a) the obligations of the person in charge and the person in charge according to articles 8,

11, 25 to 39, 42 and 43; (…)"

In this regard, the LOPDGDD, in its article 71 "Infractions" establishes that

"The acts and behaviors referred to in sections 4,

5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that result

contrary to this organic law".

For the purposes of the limitation period, article 73 "Infractions considered serious"

of the LOPDGDD indicates:

"Based on what is established in article 83.4 of Regulation (EU) 2016/679,

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

substantial violation of the articles mentioned therein and, in particular, the

following:

(…)

r) Failure to comply with the duty to notify the data protection authority

data of a breach of security of personal data in accordance

with the provisions of article 33 of Regulation (EU) 2016/679. (…)”

Without prejudice to the provisions of article 83.5 of the GDPR, the aforementioned article provides in

its section 7 the following:

fourteenth

“7. 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.

For its part, 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

autonomous communities 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.

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. (…)”

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: IMPOSE the MINISTRY OF HEALTH, with NIF S7800001E,

-For an infringement of Article 5.1.f) of the GDPR, typified in article 83.5 of the

GDPR, a warning sanction.

-For a violation of Article 25 of the GDPR, typified in article 83.4 of the GDPR,

a warning sanction.

-For a violation of Article 32 of the GDPR, typified in article 83.4 of the GDPR,

a warning sanction.

-For a violation of Article 33 of the GDPR, typified in article 83.4 of the GDPR,

a warning sanction.

SECOND: NOTIFY this resolution to the MINISTRY OF HEALTH.

THIRD: COMMUNICATE this resolution to the Ombudsman, in

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

938-120722

C / Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es