 File No.: PS/00233/2021

RESOLUTION OF PUNISHMENT PROCEDURE

Of the procedure instructed by the Spanish Agency for Data Protection (as regards
hereafter, AEPD) and based on the following

BACKGROUND

FIRST: On May 21, 2020, the director of the AEPD, following the
same criteria used before any news published in the media
communication that affects the treatment of health data by the
Public Administrations, and, given the news that appeared in the media
regarding the project of the Government of Spain about the implementation of an application
tion (or also, App) for tracking possible COVID-19 infected, entrusted to the
SECRETARY OF STATE FOR DIGITALIZATION AND ARTIFICIAL INTELLIGENCE (in
hereinafter, SEDIA), of the MINISTRY OF ECONOMIC AND TRANS-
DIGITAL TRAINING (hereinafter, the METD), which will use a program-
tion of applications (hereinafter, API) from Google and Apple, a protocol to be inter-
operable between countries, which will be launched as a pilot in the Canary Islands at the beginning of June,
connecting to the healthcare computer systems of the Autonomous Communities,
urges the Subdirectorate General of (hereinafter, SGID) to initiate the actions
preliminary investigations referred to in article 67 of Organic Law 3/2018,
of December 6, Protection of Personal Data and guarantee of digital rights
such (hereinafter, LOPDGDD), in relation to the actions carried out by the SE-
DIA, in case of such facts there are indications of infraction in the scope
potential of the AEPD.

SECOND: A.A.A. (hereinafter, the claimant party one) dated September 7
2020 files a claim with the AEPD.

He bases his claim -among other aspects- on the following circumstances:

“6. That on the date of this claim, and in accordance with the information

tion available on its website and Privacy Policy (***URL.1):

(a) App name: RadarCovid

(b) Publication date: July 7, 2020

(c) Responsible for the treatment: General Secretariat of Digital Administration,

dependent on the Ministry of Economic Affairs and Digital Transformation

However, it is not clear from the RadarCovid Privacy Policy

What is the role of the health authorities of the CCAA that have completed

technical processes to integrate into Radar COVID (eg commissioning

data subjects, data controllers, co-responsible parties,

etc.).

(d) Publication of the DPIA: No

(e) Publication of the source code: No

(f) Pronouncement of the Control Authority (article 36 and/or 57.1c RGPD):

Nope

On June 23, 2020, the AEPD clarified through a statement that:

- your involvement in the contact tracing app developed by the

SGAD had limited itself to initiating on May 21 a procedure

of previous investigative actions that have not yet concluded.

- Ignorance of the details of the practical articulation of the application

cation and the pilot experience, essential to analyze its incidence

on the privacy of citizens, has given rise to the requirement

of formal requests for information to the SGAD and has prevented

its adequacy to the personal data protection regulations with

advance.

***URL.2

(g) Legality of the treatment:

In accordance with section “10. What is the legitimacy for

treatment of your data? of the RadarCovid Privacy Policy:

- Consent: Article 6.1 a) of the RGPD.

- Legitimate interest: Article 6.1 e) of the RGPD based on national regulations.

approved for this purpose (Ministerial Order SND/297/2020 of 27

March19).

However, it should be noted that said Order only regulates the creation

tion of the application “Assistance COVID-19”, not RadarCovid, so

It would remain pending to clarify the national legislation that . Article 9.2 i) and

j) of the RGPD.

(j) Purposes of the treatment:

In accordance with section “5. For what and why do we use your

data?" of the RadarCovid Privacy Policy:

- The collection, storage, modification, structuring and in its

case, deletion of the data generated, will constitute operations of

treatment carried out by SGAD, in order to guarantee the

proper functioning of the App, maintain the service relationship

of the service with the User, and for the management, administration, information

tion, provision and improvement of the service.

- The information and data collected through the Application will be treated

two for purposes strictly of public interest in the field of health

public, given the current health emergency situation as a consequence

incidence of the COVID-19 pandemic and the need for its control and

propagation, as well as to guarantee your vital interests or those of third parties.

zeros, in accordance with current data protection regulations.

- For this purpose, we use your data to provide you with the “Radar

COVID” and so that you can make use of its functionalities according to

do with their terms of use. In accordance with the General Regulation

General Data Protection (RGPD) as well as any national legislation

that is applicable, the General Secretariat of Di-

gital will treat all the data generated during the use of the App for the

following purposes:

. Offer you information about contacts considered to be at risk

of exposure to COVID-19.

. Provide you with practical advice and recommendations for action

tions to follow as situations of risk of

facing quarantine or self-quarantine.

- This treatment will be carried out through the alert functionality.

contagion that allows to identify situations of risk for having

been in close contact with people who use the application

are infected with COVID-19. In this way you are informed

It will tell you what steps should be taken afterwards.

5. That by virtue of Article 58 of the RGPD, the Spanish Protection Agency

of Data can make use of its investigative and corrective powers

against SGAD.

6. For all of the above, and by virtue of Article 77 of the RGPD, the

Claimant:

REQUEST THE SPANISH DATA PROTECTION AGENCY

That it considers the previous allegations to have been made for the appropriate legal purposes.

tunes, and by virtue of the powers provided for in article 58 of the RGPD proce-

gives to:

Investigate whether the RadarCovid application complies with the principles of legality, fairness,

taty, transparency and proactive responsibility of the RGPD (Article 5), in accordance

conformity with the guidelines of the EDPB (Article 70 RGPD), to the extent that

that:

(a) SGAD has not published the content of the EIPD, despite the "increased"

recommendation of the EDPB, as well as confirm if SGAD has prepared the

EIPD and, where appropriate, raised the prior consultation with the AEPD before

protect the processing of personal data (Article 35 and 36 RGPD);

(b) SGAD has not published the source code, as required by the EDPB in

its guidelines;

(c) SGAD has not defined in the Privacy Policy the functions and responsibilities

bilities of the health authorities of the Autonomous Communities that have completed

the technical processes necessary to integrate the application into their systems.

more sanitary (Article 13 and 14 RGPD);

(d) SGAD has not specified clearly enough the different financing

lities of the treatment and their respective legitimizing bases, in attention

to the provisions of section “5. For what and why do we use your data?

cough?" and “10. What is the legitimacy for the treatment of your data? of

the Privacy Policy (Article 13 and 14 RGPD); Y

(e) SGAD has not specified the data retention periods for fi-

scientific or historical research or statistical purposes in the Policy

of privacy (Article 9.2j and 89.1 RGPD).”

On said claim fell resolution of ADMISSION TO PROCESS dated 5 of

October 2020, in the file with no. of reference E/07823/2020.

On January 24, 2021, claimant one, expands his claim and

transfers to the AEPD some complementary allegations based -among others

aspects-, in the following circumstances:

1. Incorporate said SUPPLEMENTARY ALLEGATIONS into the investigation

that the AEPD is carrying out due to a possible violation of the regulations

in terms of data protection;

FIRST: Late and incomplete publication of the source code

That on September 9, 2020, the SGAD published the source code

of the RadarCOVID application, accessible online through the Gi-

tHub, as communicated by the SGAD through its official Twitter account.

However, the same day after the release of the code, some media outlets

communication echoed the discomfort of the development community

res, to the extent that:

- the code was obfuscated and

- the history had not been published; essential aspects to be able to

analyze it and that it did not occur in the repositories of the applications

Italian or German nes published since May 2020.

In the context described, this Part understands that the publication of the code

RadarCOVID source was late and incomplete, made incompatible new-

with the principles of transparency and proactive responsibility of the arti-

Article 5 of the RGPD, in response to the interpretation made by the Committee

European Data Protection Agency (hereinafter, “EDPB”) in its Guidelines

04/2020.

SECOND: Modification of the data controller

Thus, through the aforementioned Agreement, on October 9, 2020,

modified (i) the flow of personal data and (ii) the data controller

that, until then, was derived from the Privacy Policy of the application.

RadarCOVID tion, in particular:

- The SGAD -which initially held the role of data controller-

to- happened to have the consideration of being in charge of the treatment; Y

- The SNS (Ministry of Health) and the Health Departments of the

Autonomous Communities would be considered data controllers, without

specify -however- if they performed these functions as correspond-

controllers (Article 26 of the RGPD) or independent data controllers.

you.

In the context described, this Party understands that in the course of the claim

mation must:

1. Verify if the following aspects are in accordance with the regulations of

Data Protection:

the legal basis that legitimized the change of person in charge of the

a)

treatment of the data obtained and processed through the application

RadarCOVID tion;

the regulation of data processing in the Conventions of

b)

Collaboration signed with each Autonomous Community; Y

c)

the fact that the aforementioned Agreement between the Ministry of

Health and the Ministry of Economic Affairs and Transformation

Digital, does not contain the specifications provided in the article

28.3 of the RGPD for those in charge of the treatment or, where appropriate,

the specifications of article 26 of the RGPD for the corresponding

treatment sabers.

THIRD: Security breach

In accordance with the information published by EL PAÍS on the 22nd of

October 2020, the RadarCOVID application would have had a breach of

security since its launch. According to the aforementioned medium, the SGAD

reported the security breach to the AEPD during the week of the 5

October 2020:

European and Spanish legislation obliges the Government to notify the

Spanish Data Protection Agency (AEPD) and to the public the existence

of a gap. The information to the AEPD was made, according to Secretarial sources,

State House, "the week of October 5." That communication was not made

It was carried out according to a procedure established by law for serious cases, but the

AEPD confirms for its part that this communication occurred in some way

mode. The level of notification, according to AEPD sources, is something that must be

Assess each data controller according to what the Regulation says

Data Protection. This is what the Secretary of State did: “The vulnerability

information was not made public because there has been no record of a violation of

the security of personal data, as set forth in article 33 of the Re-

regulation”, say official government sources. According to his criteria, there would be ac-

dressed correctly.

In the context described, this Party understands that during the course of the

claim must be confirmed if:

1. There was indeed a security breach in the terms

indicated by the AEPD in its Guide for the management and notification of

security breaches; Y

2. If applicable, if the breach was notified to the AEPD and/or the interested parties,

in accordance with the provisions of articles 33 and 34 of the RGPD.

FOURTH: Data communications to the “EU interoperability gateway”

That since last October 30, 2020, the RadarCOVID application is-

It is connected to the interoperability node of the European Commission, as

as published by the SGAD through its official Twitter account and indicated

in the content of the application itself:

That in accordance with the information published by the European Commission

in the document “National Joint Controllers and Privacy policies”, in the case

of Spain, the co-responsible for the treatment that carries out the communications

tions of the data obtained through RadarCOVID to other applications of

tracing in the European Union within the framework of the “EU interoperability Gateway

for contact tracing and warning apps” is: General Directorate of Public Health

ca, Support Unit, Ministry of Health.

In the context described, this Party understands that during the course of the

processing of the claim, it must be confirmed whether the General Directorate

of Public Health, Support Unit, Ministry of Health, in his condition

co-responsible for the processing of the interoperability node, complies with

the fundamental issues set by the EDPB in its Declaration on

the impact on data protection of the interoperability of applications

contact tracing and, in particular, on the security and information

information and the need to carry out an impact assessment on the

data protection (hereinafter, “EIPD”) in accordance with article 35

of the GDPR.

It should be remembered that, as this Party made clear in its re-

claim of the past 09/07/2020, in the case of RadarCOVID and as of the date of

present writing, the EIPD has not yet been published, as recommended in-

lackingly the EDPB in its Guidelines 04/2020.

FIFTH. Modification of the RadarCOVID Privacy Policy

This Party observes that they have included modifications in the Privacy Policy

RadarCOVID application with respect to the version published in the mo-

moment to make the claim on 09/07/2020, accessible through

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

7/168

of the following link: ***URL.3 (hereinafter, “Current Privacy Policy”).

1. A new section has been added -which did not appear in the previous version- ti-

entitled “Who are responsible for the treatment of your data as

user of “Radar COVID”?”, in which it is established:

3. Who are the controllers of your data as

user of “Radar COVID”?

This application is responsible for processing both the Ministry

Ministry of Health, as well as the Autonomous Communities. Likewise, the

General Secretariat of Digital Administration is in charge of the

treatment.

At the national level, the person responsible for processing your data as

“Radar COVID” user is:

As part of the COVID-19 contagion alert system, it is processed

The following data will be used for users who have tested positive for CO-

VID-19 for the purposes specified below:

- Name: Ministry of Health.

- Address: Paseo del Prado 18-20, 28014 Madrid

The General Secretariat of Digital Administration, as head

of the application and based on the order of the treatment entrusted

by the Ministry of Health, will carry out the following operations of the

treatment:

-Generation of codes for the communication of positives in the appli-

COVID Radar cation.

- Reception of the information sent by users when they communicate

They don't have a positive. This information includes: (i) The exposure keys

daily up to a maximum of 14 days. The exact number of keys

communicated will depend; (ii) The preference or not to communicate these

daily exposure keys to the European interoperability node in-

three contact tracing apps.

- Composition of an updated list of temporary exposure keys

portal that are made available for download by

Radar COVID applications.

- In relation to the European contact interoperability node

(EFGS):

(i) Daily receipt of exposure key listings

generated by the national servers of the States

Member States adhering to the project, where applicable; Y

(ii) Daily submission to the EFGS node of a list of passwords

temporary exhibition submitted by users of Radar CO-

VID who have explicitly consented to share this information

communication with the rest of the Member States adhering to the

project.

The Autonomous Communities adhered to the use of the application are, as well

same, responsible for the treatment, carrying out the following operations

treatment tions:

Request to the Radar COVID server for the generation of

-

positive confirmation.

Delivery of these codes to people diagnosed positive

-

You go for PCR tests.

The person in charge of the treatment and owner of the application is the General Secretariat.

Directorate of Digital Administration, directive body of the Secretary of State for

Digitization and Artificial Intelligence of the Ministry of Economic Affairs and

Digital Transformation, under the Agreement between the Ministry of Foreign Affairs

Economics and Digital Transformation (Secretariat of State for Digitization

tion and Artificial Intelligence) and the Ministry of Health about the application

“Radar COVID” tion.

2. Regarding the section "What data do we process about you?", part has been modified

of the applicable legislation that was listed for the purpose of legitimizing the

data processing: (...)

3. Regarding the section “Who has access to your data?”, the

affirmation that RadarCOVID does not process personal data, since it re-

It is evident that the application treats pseudonymized data, subject to the norm

data protection requirement: (...)

However, in the application itself, users are offered information

erroneous statement indicating that RadarCOVID does not process any type of personal data.

end: (...)

4. Regarding the section “What are your rights and how can you control your

data?”, the mention that the RadarCOVID app does not al-

stores personal data and, therefore, the rights of

access, rectification, deletion, limitation, opposition and portability: (...)

5. A new section has been added -which did not appear in the previous version of

the Privacy Policy- entitled "Transfer of data to countries of the

European Union”, which establishes: (…)

In the context described, this Party understands that during the course of the processing

tion of the claim, it must be confirmed if, after the modifications included in

the Privacy Policy, RadarCOVID provides interested parties with all the information

required by article 13 of the RGPD, in particular:

1.

The identity and contact details of the Departments of Health

of the Autonomous Communities, in its capacity as responsible for the

treatment (article 13.1 “a” of the RGPD);

The contact details of the Data Protection Delegate of all

two.

two data controllers (article 13.1 "b" of the RGPD);

3.

The purposes of the treatment to which the personal data is destined and

the legal bases of the treatment (article 13.1 “c” of the RGPD). In particular

lar, regarding compliance with:

a) The EDPB guidelines (…) 9, 10, 11 and 12

b) Article 27 of Royal Decree-Law 21/2020, of June 9, of me-

urgent prevention, containment and coordination measures to make

in the face of the health crisis caused by COVID-19, referenced

in the RadarCOVID Privacy Policy: (...)

4. Regarding the existence of the right to request the data controller

access to personal data relating to the interested party, and its rectification

deletion or deletion, or the limitation of its treatment, or to oppose the treatment-

treatment, as well as the right to data portability (article 13.2

“b” of the GDPR). In particular, regarding compliance with what is indicated by

the EDPB in its Declaration on the impact on data protection of

the interoperability of contact tracing applications: (…)

In the previous version of the RadarCOVID Privacy Policy, it was in-

indicated that it was not possible to exercise the rights with the following

statement “Since the Radar COVID app does not store personal data,

rights, the rights of access, rectification, su-

pressure, limitation, opposition and portability, as well as not to be subject to

decisions based solely on the automated processing of your

data".

However, and in accordance with the new wording of the clause,

seems to infer that, at present, the exercise of rights is allowed

rights (except the right of portability and the right not to be subject to

based solely on automated processing):

In the described context, it is in the interest of this Party to confirm whether:

a) In attention to the operation of the RadarCOVID application and

to the treatment of the use of pseudonymized data, it is possible to identify

notify the interested parties and, therefore, it is possible to exercise

the rights according to the EDPB;

b) Where appropriate, provide means that allow the exercise of

rights through a legal and voluntary representative, in accordance

with article 12.1 of Organic Law 3/2018, of December 5,

bre, Protection of Personal Data and guarantee of the rights

digital (hereinafter, “LOPDGDD”);

c) If applicable, indicate the means by which the interested parties

can exercise their rights before the Departments of Health of

each CC.AA. (in their capacity as data controllers),

in accordance with article 12.2 of the LOPDGDD. (…)

2. Extend the claim to the new data controllers.

the RadarCOVID application identified in it (i.e. Ministry of Health and

Departments of Health of the corresponding Autonomous Communities and Cities

nomic) for holding these the passive legitimation in the present procedure;

3. Where appropriate, order those responsible or in charge of Ra-

darCOVID that treatment operations comply with the provisions of the

GDPR, when applicable, in a certain way and within a specified period.

cified, in accordance with the express guidelines and interpretations made

given by the EDPB on the matter; Y

4. If applicable, sanction anyone responsible for or in charge of Ra-

give COVID with warning when the treatment operations have in-

infringed the provisions of the RGPD, in accordance with the express guidelines and

interpretations made by the EDPB on the matter."

THIRD: B.B.B. together with ten more professors (hereinafter, the claimant two),

dated October 1, 2020 files a claim with the AEPD, with the

following tenor:

"We hereby inform you of a security breach in the App Radar

COVID, reported to SEDIA and Indra S.A, on September 16, 2020. Ad-

we put together the technical report as well as the legal assessment in the legal note that

we send Vice President P.P.P. and the Secretary of State C.C.C. this lu-

It's September 28."

On said claim fell resolution of ADMISSION TO PROCESS dated 5 of

October 2020, in the file with no. of reference E/07905/2020.

FOURTH: A natural person ***CLAIMAN.3 (hereinafter, the claimant party

three) dated October 5, 2020 files a claim with the AEPD.

In particular, it reports how a design decision in the tracking application

contacts Radar COVID puts the privacy of its users at risk.

"Specifically, the risk comes from only COVID-positive users uploading

the TEK keys (keys with the result of a test) to the radar server-covid-backend-

dp3t-server (***URL.4, with IP ***IP.1, ***IP.2, ***IP.3, ***IP.4 accessible via

CloudFront CDN). Therefore, every time a key upload is observed from

a phone to the endpoint ' /v1/gaen/exposed ' of this server, it can be inferred that the

phone owner is COVID-positive. The encryption between the application and the server

vidor does not help to cover up that information: even if the endpoint and the content of the

rise are not observable, the length of the messages will reveal a rise in class.

go TEK to the server."

On said claim fell resolution of ADMISSION TO PROCESS dated 16

October 2020, in the file with no. of reference E/08295/2020.

FIFTH: RIGHTS INTERNATIONAL SPAIN (hereinafter, claimant four)

dated February 26, 2021 files a claim with the AEPD.

In particular, it bases its claim on the following circumstances:

"- After becoming aware of the processing, by this Agency, of a pro-

ex officio proceeding investigating the contact tracing application Radar CO-

VID, and having detected a series of potential risks for privacy and

non-compliance with the applicable guidelines, the RIGHTS INTERNATIONAL association

NAL SPAIN submits a document for incorporation into the procedure, in which

irregularities are denounced with respect to the publication of the application code

tion.

- In this sense, attention is drawn to the fact that, despite being able to

be downloaded the application in various Autonomous Communities (it is even licensed

released a version for a pilot project), the code was not published until 9

September 2020, and the same differed from the one that the application had in its initial version.

cial. In addition, to date, the history of the development of the

app, that is, the history with all the data and steps that have been taken since the

beginning of its development.

- In relation to the pilot, the association criticizes that, since the

source code, its exact scope is unknown, although downloads are not

were geolocated, and, therefore, the app could be downloaded and installed

from any geographical area. The indices used to quantify the success of

the action went beyond the territory delimited for the tests, and could affect

to users not informed or aware of the use of information from their terminals

- The association considers that the aforementioned lack of transparency caused

a delay in detecting a breach of personal data in the app, since,

as it was later discovered, it only sent information to the server in case of

detect a positive.

- Finally, the association draws attention to some relative deficiencies

to the Impact Assessment document, which was recently published, in January

2021, even though the app was available as early as June 2020.

According to their change control, the published version is the November 2020 version, not

indicating anything about previous versions, changes made, and

the risks that may have been detected after the evaluation

initial. They question the usefulness of an impact assessment presented and elaborated

give it this way."

On said claim fell resolution of ADMISSION TO PROCESS dated 12 of

March 2021, in the file with no. of reference E/02649/2021.

SIXTH: Within the framework of the previous investigation actions, five

information requests addressed to SEDIA and one to the General Secretariat of

Digital Health, Information and Innovation of the National Health System (hereinafter,

SGSDII).

In the request addressed to the SGSDII, dated December 4, 2020, it was requested-

ba the following information:

Within the framework of the reference inspection actions, initiated ex officio

by the Spanish Data Protection Agency in relation to the news appearing

received in the media about the Government's project to implement

tion of a bluetooth tracking app of possible COVID-19 infected,

has been requesting since May to the Secretary of State for Di-

digitalization and Artificial Intelligence information and documentation in relation to

this app.

The representative of the SGAD states, in a letter dated September 1,

2020, regarding the "RADAR COVID" app that the Ministry of Health has the

condition of data controller, and each Autonomous Community will be

responsible for processing the data in their respective field, while

the General Secretariat of Digital Administration (Secretariat of State for Digitali-

tion and Artificial Intelligence has the status of data processor).

On October 13, 2020, the "Agreement between the Ministry of

Economic Affairs and Digital Transformation (Secretariat of State for Digitali-

tion and Artificial Intelligence) and the Ministry of Health about the application

"RADAR COVID" published in the BOE of 10/15/2020, whose purpose is:

a) Delegate to the General Secretariat of Digital Administration (in addition

before, SGAD) of the Ministry of Economic Affairs and Transformation

Digital, all the skills of design, development, implementation and

evolution of the "RADAR COVID" application that correspond to the Di-

General Directorate of Digital Health and Information Systems for the

National Health issue under the provisions of article 8.2.a) of the

Royal Decree 735/2020, of August 4, which develops the es-

basic organic structure of the Ministry of Health, the General Secretariat

ral of Digital Health, Information and Innovation of the National System of

Health. The General Secretariat of Digital Health, Information and Innovation

of the National Health System has previously approved the delegation

of all these powers in the SGAD in accordance with the provisions of

Article 9.1 of Law 40/2015, of October 1.

b) Delegate to the SGAD the competence of the Minister of Health to

sign with the autonomous communities and cities the agreements of

collaboration for the adherence of these to the use of the application "RADAR

COVID", in accordance with the provisions of Chapter VI of the Preliminary Title

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

Public. without prejudice to the support that to facilitate its processing

The General Secretariat of Digital Health, Information and Innovation will

of the National Health System.

The descriptive part of the Agreement includes the following in the sixth point:

"Sixth.- That, since May 2020, the SGAD has been developing-

with the knowledge and consent of the Ministry of Health, an application

tion for the traceability of contacts in relation to the pandemic caused

by COVID-19 called “COVID RADAR”. During the month of July

2020, with the agreement of the General Directorate of Public Health, Quality and

Innovation of the Ministry of Health, the SGAD successfully carried out the pro-

pilot project of the same, whose success guarantees the viability of the proposed solution.

set up for close contact tracing.”

Likewise, points 3 of the second and third of the clauses of the agreement are-

tablece:

3. In relation to the delegation of powers provided for in letter a) of the

first clause of this Agreement, correspond to the General Secretariat of

Digital Health, Information and Innovation of the National Health System, in addition to

more than its obligations as Responsible for the processing of character data.

ter staff, and its General Directorate of Digital Health and Information Systems

for the National Health System, the following obligations:

a) Monitoring of the design and implementation of the “Radar CO-

VINE".

b) The reception of the data held by the SGAD (related to

with your active download, use, codes used, etc.) for the ade-

when the epidemiological monitoring of the Pandemic in Spain, as well as

as its relationship with other European countries.

c) The promotion of the necessary measures for its correct application

within the scope of powers of the General Secretariat of Health

Digital, Information and Innovation of the National Health System, as well

as the impulse of the agreements that were necessary to adopt in this regard.

in the Interterritorial Council of the National Health System.

d) The analysis of the fulfillment of objectives and, where appropriate, the proposal

reformulation of procedures and indicators to adjust them to the needs

supervening cessions.

e) Any other obligations necessary for the proper functioning

ing of the application. (…)

3. In relation to the delegation of powers provided for in letter b) of the

first clause of this Agreement, correspond to the General Secretariat of

Digital Health, Information and Innovation of the National Health System, in its

condition of Responsible for the processing of personal data, give

the necessary indications to the SGAD in its capacity as data processor.

I lie.

Likewise, they correspond to the General Secretariat of Digital Health, Information and

Innovation of the National Health System and its General Directorate of Digital Health

such and Information Systems for the National Health System the following

obligations:

a) Collaboration with the SGAD and the ministries of the communities and

autonomous cities competent in the matter in all actions

necessary for the correct implementation and development of the «Ra-

give COVID.”

b) Ensure the proper functioning of the "Radar COVID" system, in

particularly with regard to the defense of the rights of the interested parties.

two.

c) Permanent monitoring of the results of the «Radar

COVID» to transfer them to the health authorities of the different

Public administrations.

d) The promotion of the necessary measures for its correct development and

execution within the scope of powers of the General Secretariat

of Digital Health, Information and Innovation of the National System of

Health, as well as the promotion of the agreements that were necessary to adopt

in this regard in the Interterritorial Council of the National Health System.

e) Any other obligations necessary for the successful completion of the

application that can be addressed from the competences of said

General Secretary.

In use of the powers conferred by article 58.1 of the Regulation (EU)

2016/679 of the European Parliament and of the Council of April 27, 2016, regarding

to the protection of natural persons with regard to data processing

personal information and the free circulation of these data and by which the Directive

tiva 95/46/CE (General Data Protection Regulation) (hereinafter RGPD),

and article 67 of Organic Law 3/2018, of December 5, on the Protection of

Personal data and guarantee of digital rights (hereinafter LOPDGDD),

It is requested that within ten business days you submit the following information

and documentation:

1. Copy, where appropriate, of the instructions given to the data processor,

and in particular in relation to data protection by design and by default.

effect of the "RADAR COVID" app.

2. Copy, where appropriate, of the reports prepared by the Protection Delegate.

tion of Data, and in particular those related to the supervision of the treatments and

to the need to prepare an impact assessment related to the protection

data tion.

3. All the information and documentation available in relation to the

measures carried out by the General Secretariat of Digital Health, Informa-

tion and Innovation of the National Health System based on the above

mentioned points 3 of the second and third clauses of the Agreement.

4. Copy of the Record of Processing Activities carried out under the res-

responsibility of the Ministry of Health. (…)

SEVENTH: In view of the allegations provided by SEDIA and the SGSDII regarding

compliance with the requirements made, the SGID issued a report on actions

previous investigations within the framework of the file with reference number E/

03936/2020, dated February 26, 2021, by virtue of investigative powers

granted to the control authorities in article 57.1 of the Regulation (EU)

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

compliance with the provisions of article 67 of the LOPDGDD, with the following tenor:

"BACKGROUND

On May 21, 2020, the Director of the Spanish Agency for Protection

Data tion agrees to initiate these investigation actions in relation to

with the news that appeared in the media about the project of the Government

government for the implementation of a bluetooth tracking app for possible infected

of COVID-19.

INVESTIGATED ENTITIES

During these proceedings, investigations have been carried out on the following entities:

Ministry of Economic Affairs and Digital Transformation - SEDIA- Secretariat of State of Digitization and Artificial Intelligence- with NIF S2833002E with address at Calle Poeta Joan Maragall 41 - 28071 Madrid.

Ministry of Health -SGSDII- General Secretariat of Digital Health, Information and Innovation of the National Health System with address in PASEO DEL PRADO, 18-20 - 28071 Madrid.

RESULT OF THE INVESTIGATION ACTIONS

1. With dates of 5/26, 8/17, 9/18, 10/2 and 10/26, 2020, the Inspectorate notified tion of Data two separate information requirements to the Secretary of State of Digitization and Artificial Intelligence requesting various information and documentation tion in relation to the mobile application (app) that will allow contact tracing by Bluetooth with the aim of early detection of possible infected by CO-VID-19 (COVID RADAR). With dates 5/6, 18/6, 3/7, 21/7, 28/7, 1/9, 22/9, 23/9, On 10/9, 10/15, 10/27, 10/30 and 11/5, 2020, respective written responses were received. by completing the information requirements made.

From the information and documentation provided, the following can be deduced:

1.1.- On October 9, 2020, the "Agreement between the Ministry of Economic Affairs and Digital Transformation (Secretariat of State for Digitization tion and Artificial Intelligence) and the Ministry of Health about the application “RA-GIVE COVID.””, whose purpose is:

a) Delegate to the General Secretariat of Digital Administration (hereinafter, SGAD) of the Ministry of Economic Affairs and Digital Transformation, all all the skills of design, development, implementation and evolution of the

"RADAR COVID" application that correspond to the General Directorate of

Digital Health and Information Systems for the National Health System

by virtue of the provisions of article 8.2.a) of Royal Decree 735/2020, of

August 4, which develops the basic organic structure of the Mi-

Ministry of Health, the General Secretariat of Digital Health, Information and

Innovation of the National Health System. The General Secretariat of Health

Digital, Information and Innovation of the National Health System has approved

previously endorsed the delegation of all these powers in the SGAD

in accordance with the provisions of article 9.1 of Law 40/2015, of October 1,

tuber.

b) Delegate to the SGAD the competence of the Minister of Health to suspend

write collaboration agreements with the autonomous communities and cities

ration for the adherence of these to the use of the "RADAR COVID" application,

in accordance with the provisions of Chapter VI of the Preliminary Title of the Law

40/2015, of October 1, on the Legal Regime of the Public Sector. without per-

judgment of the support that the Secretariat will provide to facilitate its processing

General of Digital Health, Information and Innovation of the National System

of health.

The descriptive part of the Agreement includes the following in the sixth point:

“Sixth.- That, since May 2020, the SGAD has been developing-

with the knowledge and agreement of the Ministry of Health, an appli-

cation for traceability of contacts in relation to the occasional pandemic

given by COVID-19 called “COVID RADAR”. During the month of July

2020, with the agreement of the General Directorate of Public Health, Quality and

Innovation of the Ministry of Health, the SGAD successfully carried out the pro-

pilot project of the same, whose success guarantees the viability of the proposed solution.

set up for close contact tracing.”

1.2 The representative of the SGAD states, in writing dated 9/1/2020, res-

regarding the RADAR COVID system that the Ministry of Health has the condition

responsible for the treatment, and each Autonomous Community will be res-

responsible for processing the data in their respective field, while the

General Secretariat of Digital Administration (Secretariat of State for Digitali-

tion and Artificial Intelligence) has the status of data processor.

1.3.- The "RADAR COVID" system is made up of:

• An app for mobile devices called “COVID RADAR” that collects

ge proximity identifiers of users from this and uses the interface of

application programming (API) developed by Google and Apple.

• A Web service that is made available to the governments of the Communities.

Autonomous Units (CCAA) to distribute the codes that allow the

users of the app who have tested positive in a COVID-19 test, send the

proximity identifiers of the last 14 days kept in the terminal

mobile terminal to the server.

• In addition, the health services of the Autonomous Communities must establish the procedures

methods and procedures necessary to facilitate users who have given

positive in the COVID-19 test a security code that is the key

to upload to the server the proximity identifiers that they keep in

mobile devices.

The first two have been developed by the Government of Spain with the fi-

purpose of helping prevent the spread of COVID-19 by identifying potential

Possible contacts that a person who becomes infected may have had in

the last 14 days and the third is the responsibility of the Health Service of

each CCAA.

1.4.- On June 15, 2020, it was agreed by the Secretary General of the

Digital Administration the contracting of services for the traceability of

contacts in relation to the pandemic caused by COVID 19 to Indra

Information Technologies S.L. (hereinafter INDRA). As stated in the

object of the contract included in the "Specifications of conditions for the design,

Development, pilot and evaluation of a system that allows contact tracing in

relation to the pandemic caused by covid-19" dated June 12,

2020, the implementation project would have three phases: pre-pilot phase, pilot phase

and post-pilot phase.

1.5.- The Government launched the pilot project on June 29 and ended on July 29

2020 on the island of La Gomera in coordination with the Government of Canada.

rias, with the Government of the Cabildo de La Gomera and with the City Council of San

Sebastián de La Gomera, as well as with the Canary Islands Health Service.

Subsequently, the Autonomous Communities have been incorporated into the project.

but in the testing phase until the signing of the agreement to be signed with each one

of them, on the following dates: Andalusia, Aragon, Cantabria and Extremadura.

ra on August 19, Canary Islands and Castilla y León on August 20, Balearic Islands on August 24
August, Murcia on August 25, Madrid and Navarra on September 1, La
Rioja on September 3, Asturias on September 4, Com. Valencian on 8
September, Melilla and Galicia on September 14, Castilla-la Mancha on September 18
September, Basque Country on September 21, Ceuta on September 24,
2020.

The implementation and use in tests throughout the national territory of the application
cation is covered by an Agreement of the Interterritorial Council of the System
National Health Council adopted on August 19, 2020, with the sequence
temporary agreement with SEDIA.

Regarding the principles of proportionality, purpose limitation, as well as
as minimization of the data collected according to the intended purposes.
you.

1.6.- They state that the main purpose of the application is to allow alerting
People who have been in contact with someone infected with COVID-
19 and inform them of the measures that should be taken afterwards, such as submitting
self-quarantine or diagnostic tests, or provide counseling
advice on what to do if you experience any symptoms. That is,
therefore, useful both for citizens and for public health authorities.
public. It can also play an important role in managing
confinement measures during possible de-escalation situations.

1.7.- They state that only the data required is collected
for the indicated purposes.

Neither the exact time nor the place of storage is carried out.
touch, however, they consider it useful to store the day of the contact to know if
occurred when the person was experiencing symptoms (or forty-eight hours

ras before) and define more precisely the follow-up message in which

advice is offered relating, for example, to the duration of the auto

quarantine.

1.8.- Regarding whether the measure is necessary, in the sense that there is no other

more moderate for the achievement of such purpose with equal efficiency,

party:

“It is very important to consider the real usefulness, necessity and effectiveness of

this Application, as well as its impact on the broader social system, including

fundamental rights and freedoms, considering that these applications

tions set a precedent for the future use of similar invasive technologies.

homes, even after the COVID-19 crisis.

The emergency situation cannot lead to a suspension of the right

fundamental to the protection of personal data. But, at the same time, the

data protection regulations may not be used to hinder or limit

assess the effectiveness of the measures adopted by the competent authorities,

especially the health ones, in the fight against the epidemic, since it

provide solutions that make it possible to reconcile the legal use of personal data

with the necessary measures to effectively guarantee the common good.

The grounds that legitimize/make such processing possible are the necessity

need to attend to missions carried out in the public interest, as well as that of

guarantee the vital interests of those affected or of third parties

nas, by virtue of what is stated in Considering 46 of the RGPD, where it is re-

knows that in exceptional situations, such as an epidemic, the legal basis

of the treatments can be multiple, based both on the public interest,

as in the vital interest of the interested party or another natural person.

The processing of personal data should also be considered lawful when

is necessary to protect an interest essential to the life of the data subject or

that of another natural person. In principle, personal data should only be

be treated on the basis of the vital interest of another natural person ***CLAIM-

TE.3 when the processing cannot be manifestly based on a basis

different legal. Certain types of treatment can respond to both motivations

important interests of public interest as well as the vital interests of the interested party,

such as when the processing is necessary for humanitarian purposes,

including the control of epidemics and their spread, or in emergency situations.

humanitarian agency, especially in the event of natural disasters or

human.

Therefore, if we proceed to make a judgment of necessity, that is, certain

decide if the treatment is necessary, in the sense that there is no other alternative.

goes less invasive to privacy to achieve this purpose with the same

efficiency or with reasonable efficiency, it should be noted that the legislation

sector in health matters does not currently have sufficient instruments

ciently precise that would allow facing a situation such as the crisis

health in which the country is still immersed.

In this sense, specific measures have been approved, such as the development

of an application such as the one being evaluated, which reinforce the instruments

coordination and cooperation in public health matters in sight

of the global characteristics of the epidemic.

1.9.- Regarding proportionality, they add:

“In this case, the benefit will have to be measured in terms of a lower proportion.

payment of the infection in global terms, with the possibility of recovering

freedom of action, and protection of the health of individuals. The data

of health have a high value, so it must be prevented that, taking advantage of

the uncertainty caused by an emergency situation, abuses

by third parties that lead to situations of loss of freedom

discrimination or other damages in the personal situation of citizens.

It is therefore a matter of making an assessment of the benefits that this treatment

training promises to contribute in the fight against the pandemic and the costs in the

privacy of individuals they may carry.

Regarding the possible damages or threats that an application

cation like this for privacy will have to take into account how it has been

carried out the application that we are evaluating and what its objectives are.

These threats may appear due to the urgency to offer solutions in

operation that relax controls and requirements to protect data

of the citizen. For example, possible threats to the

privacy in its implementation. On the other hand, we must not forget

that an app or a web is only an interface to display and bring data to

A server.

The main threats to the privacy of this type of solutions come from

the realization of maps of relationships between people, reidentification by
implicit calization, of the fragility of protocols when building “cards
tas” almost anonymous, and to disperse the signs of contagion in such a way that
the identity of those infected is not identified in any case. must have
Keep in mind that the treatment of the information not only affects the user of the
application but also that of all third parties with whom it has been in contact.
touch, so this treatment must comply with the principles of protection of
data.
There are studies on the robustness of cryptography and anonymization protocols.
tion (see attached document 12. DP3T - Data Protection and Security), and always
pre there is a possibility that applying sufficient time and capacity of
computer can break down and associate anonymous nicknames with phone numbers.
phone and people. From a privacy point of view, the more calculations
is done on the server side, the less control users have, so
that centralized solutions always seem less respectful of the
privacy than those distributed. The possibility that, due to the accumulation
data centrally, an abuse occurs in a company
unethical, the purposes of the treatment will be expanded or if you were a victim of
a cyber attack constitutes another of the greatest threats of this type of solution.
tions.
Regarding the benefits that this type of treatment can represent, it is
It is important to bring up the analysis carried out by the AEPD itself on whether the
The use of these data represents an important benefit in the pandemic crisis.
determining that the success of this type of solutions is based on many
many factors that do not depend on technology. First of all, it is necessary
would involve the involvement of a large number of users, some studies speak

of at least 60% of a population which, taking into account children and

the elderly account for almost all mobile users. On the other hand, depending

that a responsible statement be made about the personal situation of

infection, preferably supervised by a professional to avoid strategies

misinformation scams. Finally, it is necessary to have access to test,

not only for all users, but to be able to update the information required

periodically and so that those who are notified of having been in

contact with an infected person can test promptly.

However, and always under a respectful use with the privacy of the users.

rios, the following benefits can be deducted:

Benefits for those interested

.- People who have been very close to someone who turns out to be a

confirmed carrier of the virus will be informed about it, in order to break

transmission chains as soon as possible.

Likewise, they will be informed of the measures that should be adopted afterwards,

such as undergoing self-quarantine or diagnostic testing, or providing

advice on what to do if you experience this or that symptom.

.- The installation of the application on the device is voluntary, without consequences.

any negative opinion for those who decide not to download or use the application.

.- The user maintains control of their personal data.

.- The use of the Application does not require tracking the location of the

individual users; instead proximity data is used

.- The information collected is stored in the user's terminal equipment and is only

collect pertinent information when absolutely necessary.

Benefits for the Administration

.- People who have been very close to someone who turns out to be a

confirmed carrier of the virus will be informed about it, in order to break

transmission chains as soon as possible.

.- Simple technology.

.- The personal data protection regulations contain a regulation

for the use of cases such as the treatment carried out with this

Application, which reconciles and weighs the interests and rights in contention for

the common good.

.- It plays an important role in the management of confinement measures.

during possible de-escalation situations.

.- It is not necessary for an authority to store real contact information.

.- Its impact can be reinforced by a strategy that favors the

expanding testing to people with mild symptoms.

Alternatives to treatment and why they have not been chosen:

In conclusion, it should be noted that this Application cannot replace, but

merely supplement, the manual contact tracing carried out by people

qualified health professional, who can determine if close contacts can

whether or not they lead to virus transmission.

This tracking task is complex, mainly because it requires professionals to

health professionals have quick and reliable information on the contacts of the

patients, so it can be concluded that the use of this Application meets

with the principles of suitability since the evaluated treatment achieves the objectives

proposed objectives and the judgment of necessity since, currently, there is no other

less intrusive alternative to privacy to achieve this purpose with

equally effective or reasonably effective.

The application is constituted as a complementary tool of the techniques

traditional contact-tracing techniques (particularly from interviews with

infected people), that is, it is part of a public health program of

greater range and the objective is that it be used exclusively until the moment

moment when manual contact tracing techniques can manage

alone the volume of new infections."

Regarding the specific purposes of the app and data processing

personal:

1.10.- They state that the objectives pursued with this alert application

of infections are as follows:

• Preserve public health without giving up the privacy of citizens.

•

Stay one step ahead of COVID-19 by proactively alerting people

You are at risk of incubating the virus.

• Minimize the economic impact of COVID-19, by controlling the pandemic

without drastic measures and facilitating the movement of people.

The main functionality of the application is to allow people to be alerted

who have been in contact with someone infected with COVID-19 and report

them of the measures that should be adopted later, such as submitting to an auto
quarantine or diagnostic tests. The ultimate goal is that people
who have been in close proximity to someone who turns out to be a confirmed carrier
of the virus are informed about it, in order to break the chains of
transmission as soon as possible.

1.11.- The mobile application implements a contact alert version
(“contact tracing”) in accordance with the “Decentralized Privacy-Preserving” protocol.
ving Proximity Tracing” (DP-3T), making use of the API developed jointly-
mind by Apple and Google of this protocol, through what is known as API
“Exposure Notification”. The app does not geolocate the user or allow tracking
of their location, but is based on the exchange of pseudo-identifiers
random, anonymous, and ephemeral data between the user's device and other phones.
us nearby mobiles, all via Bluetooth low energy. Neither does the app.
requires the identification or login process, nor does it request any personal data.

According to this protocol, when a person tests positive for
COVID-19 and decide to share this data, only the
anonymous pseudocodes that he has issued and not those that he has detected from others
nearby mobiles, unlike the centralized model that sends everyone. For the
Therefore, the collation and analysis of data is carried out on the mobile of each user
and not on the server.

Regarding the types of data collected from users

1.12.- The application does not require registration and does not ask the user for any data
personal character, they are only stored in the user's terminal equipment
pseudo-random codes or Proximity Identifier, which are data generated
generated by exchanging Bluetooth low energy signals
(BLE) between devices within a relevant distance from the point of

epidemiological point of view and for a relevant time also from the point of

epidemiological view.

The app does not collect location data.

These proximity identifiers are communicated only when

confirmed that a user in question is infected with COVID-19 and on condition

tion that the person opts for this to be done. These proximity data

are generated through the Google and Apple APIs without reference to any

user or device data.

Regarding the planned retention period for the data:

1.13.- The proximity data will be deleted when they are no longer necessary

to alert people and at the latest after a period of one month (period-

incubation rate plus margin).

The data is stored on the user's device, and only those that have

have already been communicated by users and that are necessary to comply with the

purpose are uploaded to the central positive validation server available.

health authorities when such an option has been chosen (i.e.,

only the data would be uploaded to the "close contacts" server of a

person who has tested positive for COVID-19 infection).

The application does not request personal data and the data of keys infected al-

stored on the server, they will be kept for the duration of the crisis

of COVID-19.

Regarding the forecast of use of the app in terms of obligation and

scope

1.14.- Downloading the app is voluntary, the user can turn off the Blue-

tooth and uninstall it at any time.

The app will be available on devices with iOS operating system, from

version 13.5, and Android, from version 6.0 and later, whichever is

tima that covers 99% of smart mobile phones, according to the share of

market published by specialized magazines.

The app warns that those under 18 years of age will not be able to use the services available.

available through the App without the prior authorization of their parents, guardians or

legal representatives, who will be solely responsible for all

acts carried out through the App by minors in their charge.

Regarding the tracking and alert procedure:

1.15.- The identifier generation procedure follows the implementa-

tion of the DP-3T protocol in the “Exposure Notification” API of Apple and Google.

Ephemeral tokens are rotated every 10-20 minutes, and are discarded when

after 14 days.

1.16.- Notification alerts only present information about: the weather

of exposure, the date it occurred, and the level of severity, on a scale

high and low. It comes as an in-app notification, which you can

be consulted at all times through the notification history.

At no time are personal data offered about the person with whom

contact was maintained.

1.17.- The procedure by which an infected positive is communicated

of COVID-19 is as follows:

1.- The patient performs a test through their Public Health Service.

2.- If the test result is positive, the health service informs

of the detection of a positive and a unique one-time key is requested.

3.- A positive confirmation code is generated that is communicated to the

authorized health officer.

4.- When the patient receives a positive result in the Covid-19 test,

You are provided with the one-time confirmation code, which you can enter

put in your App.

5.- With the patient's consent, his phone sends the confirmation code

one-time signature, which is verified by the server, and the his-

Toric the last 14 days of Bluetooth keys on the central server.

Regarding the treatments carried out by the Autonomous Communities:

1.18.- The Autonomous Communities, as data controllers in their respective field,

They are responsible for providing a code (12-digit PIN) to customers.

patients who are positive in the PCR test for COVID19 and who have the

RADAR COVID app installed on your mobile device. In this sense, from

the centralized alert management system a web service has been enabled

from which a set of codes is made available to the Autonomous Communities

sites. From there, each CCAA must define a custody procedure and

distribution of those positive codes to patients diagnosed with CO-

VID19 guaranteeing the custody of these codes and their distribution according to

to the procedure defined in each CCAA by virtue of its competences in the

healthcare field.

1.19.- The sending of positive identifiers between the central server and the Autonomous Communities

does not use certificates, but key pairs (public-private) that are generated in

the CCAAs. The Autonomous Communities include a JWT token in the request (procedure that

enables the authentication process between an identity provider and a

service provider through a URL, which they generate signed with their primary key.

vada).

From the central server, the signature of the JWT token of the request is validated with the

public key that they have previously shared.

Additionally, a field containing the signature is included in the response.

base64 of the concatenation of all the supplied codes and is used to

generate said signature the private key of the server. The Autonomous Communities validate that signature

with the server's public key, which is included in the integration document.

tion, to ensure that there has been no alteration of the codes provided.

The delivery of public keys is done privately between the CCAA and the

service provider and an ad-hoc procedure will be defined in the case of

that a public key of a CCAA could have been compromised since

once a key in a CCAA is identified as having been compromised,

it can be removed from the system or replaced by another. For the same reason

there is no code revocation procedure, but it is equally possi- ble

could be deleted or expired.

Regarding the third parties involved in the treatments:

1.20.- Indra Information Technologies S.L:

The "Condition specifications for the design, development, pilot and evaluation of a

system that allows contact tracing in relation to the occasional pandemic

affected by covid-19", accepted by INDRA, includes in the object of the contract

the needs to be covered and, among others, the following clauses:

"5.4. Infrastructure in the cloud (cloud).

It will be specified that the Backend developments are carried out in an infrastructure

structure in the cloud in self-management mode, to facilitate agility

in solution development.

Notwithstanding the foregoing, both storage and any activity

Data processing authority will be located in the territory of the European Union.

ropea, whether these are provided and managed by the awarded company

taria or by its contractors and collaborators, and will be hosted on servers

and/or data processing centers of the awardee company itself or of

your contractors.

…

As far as possible, the use of components will be sought.

in the cloud infrastructure that allow the future migration of the solution

tion to the SARA cloud of the AGE.

6.1. General Confidentiality

The contractor undertakes to guarantee the strictest confidentiality

privacy and reserve on any data or information that may have

access or could know on the occasion of the execution of the contract, as well

and on the results obtained from their treatment, since only

will be used to achieve the object of the contract, they cannot

communicating, using, or transferring them to third parties under any con-

I accept, not even for its conservation. These obligations extend

give to all persons who, depending on the contractor or by

their account, have been able to intervene in any of the execution phases

tion of the contract.

The obligation of confidentiality and reserve entails that of custody and im-

request access to the information and documentation provided and to those

resulting from your treatment of any third party outside the contracted service.

Stated, understanding as such any person outside the company

sa contractor like anyone who, although not being a contractor, is not authorized

to access such information.

Likewise, the contractor undertakes to ensure the integrity of the

data, that is, to the protection of the information provided and to that which

result of its treatment against unauthorized modification or destruction

gives of the data.

6.2. Personal data protection

The provisions of organic law 3/2018, of 5 December, must be complied with.

December, Protection of Personal Data and guarantee of the rights

digital, adapted to Regulation (EU) 2016/679 of the European Parliament

peo and of the Council, of April 27, 2016, and by which the Di-

Directive 95/46/CE (General Data Protection Regulation), including

in accordance with the provisions of the first additional provision of the Organic Law

CA 3/2018, of December 5 and in Royal Decree 3/2010, of January 8

river

In accordance with the first additional provision of Organic Law 3/2018,

of December 5, Security measures in the field of the public sector

public, the security measures to be applied within the framework of the treatments

personal data will correspond to those of the Administration

of public origin and will be adjusted to the National Security Scheme.

INDRA SOLUCIONES TECNOLOGÍAS DE INFOR-

MACIÓN, SLU the express manifestation of submission to the regulations

national and European Union legislation on data protection

in accordance with articles 35.1d and 122.2 of the LCSP modified by ar-

Article 5 of Royal Decree Law 14/2019, of October 31, which establishes

adopt urgent measures for reasons of public security in matters of

digital administration, public sector contracting and telecommunications

tions.

6.3. Security

INDRA INFORMATION TECHNOLOGY SOLUTIONS, SLU

will implement the technical and organizational security measures

and will prepare the pertinent documentation, in accordance with the

corresponding risk analysis, as established in the Royal Decree

decree 3/2010, of January 8, which regulates the National Scheme

Security in the field of electronic administration.

7 INTELLECTUAL PROPERTY

Without prejudice to the provisions of current legislation on the subject of

intellectual property, the successful bidder expressly accepts that the property

ity of all the products that are made by the successful bidder, including

including its employees and, where appropriate, any subcontracted company,

in performance of the Contract and, in particular, all property rights

intellectual and/or industrial property derived from them, corresponds

only to the contracting administration, exclusively and without further

limitations than those imposed by the legal system.

For the purposes set forth in the preceding paragraph, the successful bidder

undertakes to deliver to the SGAD all the technical documentation

ca, works and materials generated, in whose possession they will remain at the end

zation of the Contract without the contractor being able to keep it, or obtain

copy of it, nor use it or provide it to third parties without the express authorization

SGAD, which would give it, where appropriate, upon formal request of the

contractor with expression of purpose."

They provide the following certificates issued in favor of INDRA:

o ISO 27018 Certificate of Privacy in the Cloud: Information systems

that support the business processes and information assets needed

saries for the provision of IT outsourcing services Administration,

Support, Exploitation and Infrastructure), both in physical and virtual environments.

updated cloud), according to the declaration of applicability in force on the date of

issuance of the certificate.

o ISO 27001 Information Security Management System Certificate

tion: The information systems that support business processes and

information assets necessary for the provision of outsourcing services

IT sourcing Administration, Support, Exploitation and Infrastructure), so-

to physical environments such as virtualized cloud), according to the declaration of

applicability in force at the date of the audit.

o STI-0014/2009 Certificate of Technology Service Management System

Information Technologies: The SMS of IT outsourcing services Admi-

nistration, Support, Exploitation and Infrastructure), both in physical environments

as virtualized cloud), according to the catalog of services in force. Certifi-

cation of the Information Technology Service Management System.

For the management of the RADAR COVID system, INDRA has contracted the services

vices of Amazon Web Services INC.

For the management of the RADAR COVID system, INDRA has contracted the services

of Amazon Web Services INC.

1.21.- Amazon Web Services INC:

- Amazon Web Services (AWS) is a set of services that offers

Amazon Web Services INC, including but not limited to server services

virtual cloud storage, scalable cloud storage, and database management.

relational data sets.

The AWS website reports that All AWS services are compliant

with the General Data Protection Regulation.

There is no specific contract signed between AWS and INDRA, the services

are contracted online, and it is a necessary condition to accept the conditions

tractual by clicking on the "contract the product" option. During the pro-

On-line contracting process the contracting party must choose the geographical area

where your data will reside. The contract includes, among others, the following:

you clauses:

“3.1 AWS Security. Without limitation as provided in section 10 to

its obligations contained in section 4.2, we will implement measures

adequate and reasonable compensation designed to help you secure your

content against any loss, access or accidental or unlawful disclosure.

date.

3.2 Data Protection. You will be able to specify the AWS Regions in

whose content will be preserved. You agree to keep

of your content in the AWS Regions of your choice and the transfer

of their content to them. We will not access or use

its content, except when this is necessary to maintain or provide

provide the services offered, or to comply with a provision

law or court order from a government authority. We don't

we will disclose your content to any government authority or third party

(b) as provided by section 3.3, we will move your content

from AWS Regions selected by you; except, in each case,

when necessary to comply with a legal provision or court order

official government authority. Unless it violates the law or a

court order from a governmental authority, we will give you notice of

any legal requirement or order as mentioned in this section

tion 3.2. We will only use your account information

accordance with the privacy notice, and you consent to such use. The avi-

Privacy policy does not apply to your content. “

- Applicable law:

“13.4 Applicable Law. This Agreement, as well as any controversy that

may arise by virtue of this, will be governed by the Applicable Laws, excluding

disclaiming any reference to the conflict of law rules. The Con-

United Nations Convention on International Sales Contracts

International Merchandise will not apply to this Contract.

13.5 Disputes. Any controversy or claim related to

any way with your use of the Offered Services, or any

product or service sold or distributed by AWS, will be resolved by the

Competent Courts, and you agree to the jurisdiction and venue ex-

jurisdiction of the Competent Courts, in accordance with the additional provisions

below.

(a) where the relevant AWS Contracting Party is Amazon

Web Services, Inc., the parties agree that the applicable parts

The provisions of this Section 13.5(a) are enforceable. controversies

shall be resolved through binding arbitration, in accordance with

provided in Section 13.5, instead of being resolved in court,

except that you may bring claims in a juvenile court

amount if they qualify for it. The Federal Arbitration Law and the legislation

The federal arbitration statute applies to this Agreement. There is not

judges or juries in arbitration, and review by a court of

an arbitral award is limited. However, an arbitrator may award

individual way the same compensations and measures that a tributary

nal (including precautionary or declaratory measures or compensation for

damages), and you must abide by the terms of this Agreement

like a court would. To initiate an arbitration proceeding, you

You must send a letter requesting arbitration and describing your re-

call our agent Corporation Service Company, 300 Des-

chutes Way SW, Suite 304, Tumwater, WA 98501. The arbitration shall be

made by the American Arbitration Association (AAA) under its

glas, which are available at www.adr.org or by calling 1-800-778-

7879. Payment for the presentation, administration and fees of the

arbitrator will abide by the AAA rules. we will refund

those charges for claims less than $10,000, unless the

arbitrator determines that the claims are frivolous. we will not claim

attorneys' fees and costs of arbitration unless the arbitrator determines

Make claims frivolous. You can choose that the ar-

bitrate is carried out by telephone, by means of written communications,

to, or at a location agreed upon by the parties. You and us agree

We agree that any dispute resolution procedure is

be carried out individually and not through a class action,

consolidated or representative. If for any reason the claim is

be brought to trial in court rather than arbitration.

je, you and we waive any right to a fair trial.

rare. Notwithstanding the foregoing, you and we agree that you

or we may sue in court to have

prohibits infringement or any misuse of proprietary rights

intellectual.

…”

- They state that the data from the RADAR COVID system is stored

on AWS servers located in the geographical area of Ireland. Apor-

as the document “AWS Cloud Architecture: Service Definition” elaborates

prepared by INDRA in which it is specified that the area in which the

AWS servers to serve the RADAR COVID app is located

In Ireland.

They provide a copy of a certificate issued by AWS at the request of INDRA in the

certifying that:

“The customer or partner can choose the AWS regions in which they are located.

will store its content and the type of storage. can replicate and

Back up content in more than one AWS Region. AWS does not transfer

not share or replicate your content outside of your chosen AWS Regions without

your consent unless required by law or the need to maintain the

AWS services. (for more information visit: https://aws.amazon.-

com/en/compliance/data-privacy-faq/)

Within the EU, the customer or partner can choose the following regions:

Currently operating locations: Frankfurt, Ireland, Milan, Paris, Stockholm.”

- Provide a certificate dated March 13, 2020 issued by BDO

Auditores, S.L.P., certifying that the information systems re-

indicated, all of them of HIGH category, and the services that are related

in the Annex to the certificate have been audited and found to be in accordance with

the requirements of Royal Decree 3/2010, of January 8, which regulates

the National Security Scheme in the field of Administration

electronically, as indicated in the corresponding Audit Report of the

National Security Scheme dated March 6, 2020. The annex

contains a list of 105 audited services, among which are

tran cloud services, hosting, database management, security,

backup, etc...

Regarding the information provided to users:

1.22.- They provide a copy of the different versions of the Privacy Policy of

the app that is also available at https://radarcovid.gob.es/.

The first version was published on August 7, 2020 together with the ver-

version 1.0 of the “Radar COVID” app (pilot version), in which res-

regarding data protection rights: “Given that the Radar application

COVID does not store personal data, the rights of

access, rectification, deletion, limitation, opposition and portability, as well as

not to be the subject of decisions based solely on automated processing

tion of your data. In any case, we are obliged to indicate that we assist you.

You have the right at all times to file a claim with the Agency

Spanish Data Protection (www.aepd.es).

The Privacy Policy published in October 2020 informs of the following-

you aspects:

.- What is the application and how it works.

.- Who are the controllers:

The application is responsible for processing both the Ministry

of Health, as well as the Autonomous Communities. Likewise, the Secret

General Office of Digital Administration acts as the person in charge of

I lie."

.- What data are processed:

The data handled by the application does not allow direct identification.

straight from the user or their device, and are only those necessary for the

sole purpose of informing you that you have been exposed to a situation of

risk of contagion by COVID-19, as well as to facilitate the possible

adoption of preventive and assistance measures.

In no case will the movements of the USERS be tracked, ex-

thus excluding any form of geolocation.

The IP address of the USERS will not be stored or processed.

Positive confirmation codes will not be stored along with

other personal data of users.

As part of the COVID-19 risk contact alert system

19, the following data will be processed for users who have

tested positive for COVID-19 for the purposes specified below:

either

The temporary exposure keys with which the device

of the user has generated the random codes sent (identification

Bluetooth ephemeral devices), to the devices with which the user

has come into contact, up to a maximum of 14 previous days. It is-

These keys have no relation to the identity of the USER.

RIO, and are uploaded to the server so that they can be downloaded by

Radar COVID apps held by other users. With these

keys, through processing that takes place on the phone

in a decentralized manner, the USER can be warned about

about the risk of infection from having been in recent contact with

a person who has been diagnosed with COVID-19, without the

application can derive your identity or the place where the

Contact.

A 12-digit one-time confirmation code makes it easy to

either

litigated by the health authorities to the USER in the event of a test

positive for COVID-19. This code must be entered next

by the user in the application to allow voluntary charging

taria to the server of temporary exposure keys.

either

The user's consent, if applicable, for the referral of

keys for temporary exposure to the European Interoperability Node

of contact tracing apps. All information is re-

shall be taken for strictly public interest purposes in the field of

public health, and in view of the health emergency situation decreed

day, in order to protect and safeguard an interest essential to life

of people, in the terms described in this privacy policy.

city, and according to articles 6.1.a), 9.2.a), 6.1.c), 6.1.d),

6.1.e), 9.2.c), 9.2.h) and 9.2.i)

- Applicable legislation:

o Regulation (EU) 2016/679, of April 27, 2016, regarding the pro-

protection of natural persons with regard to the processing of

personal data and the free circulation of these data and by which

repeals Directive 95/46/CE (General Regulation for the Protection of

Data).

o Organic Law 3/2018, of December 5, on the Protection of Personal Data

personal data and guarantee of digital rights.

o Organic Law 3/1986, of April 14, on Special Measures in Mathe-

Public Health ria.

o Law 33/2011, of October 4, General Public Health.

o Law 14/1986, of April 25, General Health.

o Royal Decree Law 21/2020, of June 9, on urgent preventive measures

prevention, containment and coordination to deal with the health crisis

ria caused by COVID-19.

o Agreement of October 9, 2020, between the Ministry of Ecological Affairs

and Digital Transformation (Secretariat of State for Digitization

tion and Artificial Intelligence) and the Ministry of Health about the

“COVID Radar” application.

- How the data is obtained and where it comes from:

The positive confirmation code for COVID-19 provided by the

Public Health Service. This will allow the upload to the server of the keys

times of temporary exposure with which the user's device has generated

generated the random codes sent (ephemeral identifiers Blue-

tooth) to the devices with which the user has come into contact,

up to a maximum of 14 previous days. These keys are only added

ben the server with the explicit and unequivocal consent of the USUA-

RIO, having entered a positive confirmation code by CO-

VID-19.

- For what and why the data is used:

The collection, storage, modification, structuring and in its

case, deletion of the data generated, will constitute operations of

treatment carried out by the Holder, in order to guarantee

the correct functioning of the App, maintain the service relationship

service with the User, and for the management, administration, information

mation, provision and improvement of the service.

The information and data collected through the Application will be treated

two for purposes strictly of public interest in the field of health

public, given the current health emergency situation as a consequence

incidence of the COVID-19 pandemic and the need for its control and

propagation, as well as to guarantee your vital interests or those of third parties.

zeros, in accordance with current data protection regulations.

For this purpose, we use your data to provide you with the “Radar

COVID” and so that you can make use of its functionalities according to

do with their terms of use. In accordance with the General Regulation

General Data Protection (RGPD) as well as any national legislation
that is applicable, the General Secretariat of Di-
gital will treat all the data generated during the use of the App for the
following purposes:

o Offer you information about contacts considered to be at risk
of exposure to COVID-19.

o Provide you with practical advice and recommendations for action
guidelines to follow as risk situations occur with regard to the
quarantine or self-quarantine.

The data will always and only be used anonymously for purposes
statistical and epidemiological.

This treatment will be carried out through the alert functionality
of infections that allows to identify risk situations for having been
been in close contact with users of the application who
are infected with COVID-19. In this way you are informed
It will tell you what steps should be taken afterwards.

- For how long the data is kept:

The temporary exhibition keys and the ephemeral identifiers of
Bluetooth are stored on the device for a period of 14 days,
after which they are removed.

Likewise, the temporary exhibition codes that have been communicated
given to the server by USERS diagnosed as positive by
COVID-19 will also be removed from the server after 14 days.

In any case, neither the temporary exposure codes nor the identifiers
Bluetooth ephemerals contain personal data and do not allow
identifier the mobile phones of the users.

- Who has access to the data

The data managed by the mobile application (daily exposure keys)

temporary identification and ephemeral Bluetooth identifiers) are stored uniquely

on the user's device for the purpose of being able to make calculations

and warn the USER about their risk of exposure to COVID-19.

Only in the case of reporting a positive diagnosis for COVID-19,

temporary exposure keys of the last 14 days generated in the

device, and under the explicit and unequivocal consent of the USUA-

RIO, are uploaded to the server for dissemination to all USERS

of this system.

These keys have nothing to do with the identity of the devices.

mobile devices or with personal data of the USERS of the Application.

tion.

- What are your rights and how can you control your data:

Current regulations grant you a series of rights in relation to

the data and information we process about you. Specifically, the rights

rights of access, rectification, deletion, limitation and opposition.

You can check the scope and full details of them on the page

Website of the Spanish Data Protection Agency (AEPD) here.

In general, you can exercise all these rights at any time.

any time and for free. You can contact the Responsible

Electronically, either the Ministry of Health or the Community

Autonomous unit of residence. In the case of the Ministry of Health,

you can do it through this form [by clicking on the form

links to the website of the Ministry of Health, Consumption and Social Welfare

(***URL.5)], or in person through the network of offices of

registration assistance using this application form

[link to the application form for the exercise of rights Regulation-

MSCBS General Data Protection Document]

Likewise, you have the right at all times to present a

claim before the Spanish Data Protection Agency

- How we protect your data

Those Responsible, as well as the SGAD in charge of the

treatment, guarantee the security, secrecy and confidentiality of

your data, communications and personal information and have adopted the

more demanding and robust security measures and technical means to

prevent its loss, misuse or access without your authorization. Measures

implemented security measures correspond to those provided for in the

Annex II (Security measures) of Royal Decree 3/2010, of January 8,

ro, which regulates the National Security Scheme in the field

of the Electronic Administration.

Finally, we inform you that both the storage and the rest

of the non-personal data processing activities used is-

will always be located within the European Union.

- What you should especially take into account when using "Radar COVID"

You must take into account certain aspects related to the minimum age

use of the Application, the quality of the data you provide us

tions, as well as the uninstallation of the Application on your mobile device.

vile.

Minimum age of use: to be able to use "Radar COVID" you have

You must be over 18 years of age or have the authorization of your parents and/or

legal guardians. Therefore, by registering in the Application, you guarantee the

Holder that you are older than that age or, otherwise, that you account

with the aforementioned authorization.

Quality of the data you provide us: the information you provide us

lites in the use of the services of the Application must always be

real, truthful and updated.

Uninstalling the Application: In general, there can be two situations:

tions in which the technical deactivation of the Application is carried out in

your device: 1) that you do it voluntarily, and 2) that from the Owner

to proceed to the technical deactivation of the Application on your device.

(e.g. in cases where we detect that you have breached the conditions

tions of use of the Application).

- Transfer of data to countries of the European Union:

Radar COVID participates in the application integration platform

of the European Union, so that the positive keys will be shared

with third EU countries and vice versa.

When the user's device downloads the positive keys for

analyze possible close contacts, it will also download the keys

positive from third countries adhering to the European project. This allows

will identify possible close contacts whether the user has been

visiting any of these countries as if you have been in close contact

bump with a visitor from these countries.

When the user enters a diagnostic confirmation code

positive for COVID-19, the consent of the free user will be requested,

specific, informed and unambiguous way to share your infected keys

with third countries through the European interoperability platform

pea facilitating the digital tracing of possible close contacts. the co

communication of your infected passwords to the network of European countries

two to this project is completely voluntary.

No data transfers will be made outside the European Union.

- Cookies policy

We only use technical cookies that allow the user to navigate

nization and use of the different options or services offered

cen in the Application such as, for example, accessing access parts

restricted or use security elements while browsing.

Regarding data storage and security:

1.23.- The daily passwords are stored in the mobile terminals that allow

the generation of ephemeral proximity identifiers (Rolling Proximity

Identifiers or RPI). In turn, the ephemeral identifiers received are stored.

two from nearby mobile phones. This information is stored a

maximum of 14 days.

1.24.- The server stores the passwords of “infected” people for post-

rior download by mobile applications. The data is stored

two in a relational database and for each reported positive, it is stored

will be born, the date of onset of symptoms, and the 14 daily cues taken from

the date of onset of symptoms. All this information resides on the device

mobile.

No data on the diagnostic tests performed is stored or managed.

given to any person. Beacons are collected from users who have

been diagnosed with Covid-19 but there is no relationship between these beacons and da-

specific cough of any user.

The data is stored encrypted based on the encryption algorithms defined.

two for Aurora databases (AES-256).

They provide the structure of the database and description of tables and fields,

which shows that the database does not include identifying data of

natural persons (Phone, imei, MAC, IP, etc…).

1.25.- Regarding the technical and organizational measures implemented that

guarantee the security of personal data state:

The RADAR COVID application, as well as its entire infrastructure, is part of

information systems managed through outsourcing services

IT cing of the company INDRA, for Administration, Support, Exploitation and

Infrastructure in both physical and virtualized cloud environments. as i know

has stated in the point "Regarding the third parties involved" of

this report, provide certificates of compliance with ISO standards

27018, ISO 27001 and STI-0014/2009.

1.26.- They provide a copy of the security audit report of the pilot app of

dated July 15, 2020 prepared by Minsait, technology business unit

INDRA's guidance and consultancy, in which it is specified that no

tests on the Bluetooth protocol itself and the communications carried out

by the same, and that the versions analyzed, the positive report is made

directly, not involving Health in this process as it is a

test environment, so the results presented will not apply to the new

vo system if it differs from the one checked in this environment.

After analyzing the findings obtained through the different tests carried out

cut, global security is considered Low, due to the existence

of at least one vulnerability classified as High.

Considering high severity vulnerabilities, the report concludes that:

The app makes use of weak passwords.

And between medium and low severity vulnerabilities, the report includes:

The communication channel is encrypted with protocols and algorithms.

Weak encryption mos.

1.27.- They provide the document prepared by the National Cryptologic Center

(CCN) which is the result obtained from the security audit of the application.

Radar COVID mobile tion and its connections, in order to assess its level

security and compliance. The analysis was aimed at verifying

of the level of compliance with the requirements and security measures contemplated

two in the CCN-STIC regulations. The static analysis app review

Android Radar COVID was carried out between August 20 and 21,

2020. The analysis of the connections carried out by the applications has been

subsequently performed in the production and pre-production environment. The revi-

connections in the pre-production environment has been carried out

between September 28 and October 2, 2020.

At the end of the analysis, the exposure status of the system is as follows-

tea:

• 14 vulnerabilities found.

• 4 corrected.

• 10 are pending correction:

~

3 are of MEDIUM criticality.

- The rest LOW.

The MEDIUM criticality vulnerabilities pending to be corrected affect the

lack of means of protection against the possibility of third parties engineering

reverse to the application with the intention of obtaining sensitive or manifest data.

popularize its operation, evade restrictions and/or understand the operation

internal to it.

Along these same lines, deficiencies have also been detected in the protection

of the application's communications with its backend. Are you-

deficiencies have been found during the analysis in preproduction, recommending

taking place its verification in the final environment, that is, in the backend in pro-

duction.

The result of the inspection is considered PASS: the evaluation of the safety

ity within this area has not found any quantifiable deviation that

could prevent validation against the security configuration

Dear.

The report concludes that in the review of the Radar COVID mobile application, in

terms of ICT security, no deficiencies have been found with

severity CRITICAL to prevent proper operation in the field of

cybersecurity, excluding functional analyzes and behaviors

them, without prejudice to the actions carried out by the Ministry of Foreign Affairs

Economics and Digital Transformation.

1.28.- They provide two documents called “Risk Analysis Report.

COVID 19 RADAR Service” prepared in compliance with the Royal Decree

951/2015, of October 23, modifying Royal Decree 3/2010, of October 8,

January, which regulates the National Security Scheme (ENS) in the

field of electronic administration, dated September 2020. The

first uses the ENS safeguards catalog, implemented by ***HE-

RRAMIENTA.1, the second also incorporates the catalog of safeguards of the

General Data Protection Regulation (RGPD) implemented by

***TOOL.1. From the risk analysis report that incorporates both

safeguards follows:

 The scope of the Risk Analysis includes the infrastructure that is

detailed in the document “Bluetooth App against Covid-19

v5.pdf” and that is necessary to provide the Covid Radar Service of the Sec-

Secretary of State for Digitization and Artificial Intelligence (app contact tra-

cing, backend deployed in the AWS cloud, and communications networks).

 Risk Analysis Methodology: Identification of the Development Phase

Implementation of the Adaptation Plan to the ENS and description of the tasks of the

MAGERIT methodology, used to carry out the activities and tasks of the

Risk system and description of the work performed:

- Asset Categorization

- Threat Categorization

- Categorization of Safeguards

- Estimation of the Risk State

 The assessment has been made according to the available information

on the RADAR COVID19 Information System in relation to the Di-

Mentions of Security: Authenticity, Confidentiality, Integrity, Dis-

Availability and Auditability or Traceability.

The assessment of the Covid Radar Service, due to the type of data that

treats and what is indicated in the CCN-STIC 803 Guide, the valuation in each one

of the security dimensions (Authenticity, Confidentiality, Integrity

Availability and Traceability) should be at least MEDIUM, however

However, due to the political and socioeconomic situation in which we find ourselves,

we contract caused by the Covid 19 pandemic and the impact that it would have

a security breach of the information it deals with, the Radar Service Co-

vine has been evaluated with a HIGH category.

 The relationship of threats that has been considered for the Risk Analysis

gos and that constitutes the catalog of threats implemented in a

standard in the tool ***TOOL.1 are: Natural disasters,

of industrial origin, errors, unintentional failures and intentional attacks

two.

 The assets considered are: Covid Radar Service, Mobile Phone, Re-

from Communications, App Radar Covid, Administrators / Operators,

Developers, Development and Maintenance of the App, Citizens, So-

ports, AWS Equipment, AWS Installations, Downloads Repository (APPLE

STORE), Cloud Service, Downloads Repository (ANDROID STORE).

 The degree of maturity of each of the articles of the

GDPR that must be taken into consideration.

 The value of the Potential Risk obtained from the tool ***TOOL-

TA.1 is 6.3 out of 10 (Very critical risk). The assets they present

critical risk level are: Communications networks, RADAR COVID app,

support, AWS facilities and AWS equipment.

ú The value of the Residual Risk (after applying the safeguards) obtained

tool ***TOOL.1 is 2.6 out of 10

(Medium risk). once the safeguards have been taken into account

guards implemented, the risk level of the assets is reduced

considerably, there are 12 assets with negligible risk, 1

with low risk and 1 with medium risk.

ú The value of the Objective Risk (Objective to be achieved after the

proposed safeguards) obtained from the tool

***TOOL.1 is 1.8 out of 10 (Low Risk).

For the COVID19 RADAR Service, it has been proposed to carry out the actions

necessary to minimize the residual risk so that there is no

Some asset with MEDIUM level risk. For this they have been selected

those risks that are above the value 2 and, above them,

Safeguards that were below the threshold have been identified.

value recommended by ***TOOL.1 for the National Scheme of

Security to raise them to the recommended value.

It is recommended to address a set of actions to improve the measures

currently existing security measures, in order to adjust the level of

Covid19 Radar Service risk at a LOW level. These actions have been

focused on security measures that can minimize the threats

that provide a MEDIUM level of risk in this Risk Analysis.

gosh. These actions will allow reaching the level of Objective Risk pro-

since they would increase the degree of maturity of the security measures

Authority Electronic Signature and Authentication Mechanisms. The actions pro-

put in this case are:

ú Use qualified certificates for the digital signature used

in the positive verification service.

ú Although access to the AWS console is via AWS

Multi-Factor Authentication (MFA), and therefore complies with the measure

If you want to use a second authentication factor, it is recommended

verify that the hardware cryptographic elements use algorithms

mos and parameters accredited by the CCN. In addition, it is recommended

review the access control mechanism to the Pos-Data Base

tgreSQL to conclude that it meets the high-level requirements.

1.29.- They provide the document “Impact Assessment Report on the

Data Protection of the RADAR COVID treatment” dated September

2020, whose content includes the following most relevant aspects:

 The objective of the document is to carry out the Impact Assessment related to

the Data Protection (EIPD) of the treatment carried out by the

“Radar COVID” application (hereinafter “the Application”), as required

in Regulation (EU) 2016/679 of the European Parliament (RGPD) when

the treatment entails a high risk for the rights and freedoms of the

Physical persons.

• The preparation of the report follows the guidelines established by the Agency

Spanish Data Protection Agency (hereinafter “AEPD”) in the “Guide

Practice for Data Protection Impact Assessments

subject to the GDPR”.

 Regarding the need to carry out an Impact Assessment regarding

Data Protection in the treatment evaluated, the report indicates that

there are factors that contribute to generating a high level of risk,

an EIPD must be carried out in order to determine a management scenario

appropriate risk assessment.

 Regarding those responsible, co-responsible and in charge of the treatment-

The report contains the following:

The data controller is the General Directorate of Public Health,

dependent on the Ministry of Health.

The person in charge of treatment is the General Secretariat of Administration

Digital, dependent on the Ministry of Economic Affairs and Transformation.

mation Digital, which has developed the Application.

 Regarding the Personal Data object of the treatment:

-

The application generates proximity data (exposure keys)

temporary tion with which the user's device has generated the

random codes or Rolling Proximity Identifier - RPI). It is-

All data will be communicated to the health authorities only

when it has been confirmed that a user in question is infected

status of COVID-19 and provided that the person chooses to do so

be done, that is, voluntarily.

Data through which the user is previously warned of

-

risky contact. These data allow us to estimate how many users

users are warned by the application of a potential risk of con-

tagio, without being able to trace his identity, and allows the National Service

National Health prepare the initiatives and resources necessary to

attend to users who have received the notification.

-

COVID-19.

-

Code provided by the health authorities for

allow the user to activate a warning alert. This number

of 12 digits will be provided by the health authorities to the

users of the application through Quick Response code (QR). The

Users may voluntarily enter said code in the Application.

cation to confirm the positive diagnosis and trigger the pro-

giving notice to your close contacts. this code

it is a confirmation of a positive diagnosis of a user. Exists

verification of said code to prevent any user from sending

false evidence.

-

Internet.

The day the user developed symptoms consistent with

The IP address that the device uses to connect to

These data do not allow the direct identification of the user or his

device, existing studies on the robustness of the protocols of

cryptography and anonymization, although there is a possibility that it may

They allow the identifiers to be broken down and associated with telephone numbers.

phone and people, applying enough time and computing capacity

to, although this is considered highly unlikely. On the other hand,

It must be taken into account that the treatment of the information not only

affects the user of the application, but also that of all third parties.

rivers with which he has been in contact.

 Regarding the purpose of the treatment:

- The main purpose of the App is to inform people who have

been in close proximity to someone who happens to be a confirmed carrier of the

virus, in order to break the chains of transmission as soon as possible. Of

In this way, the Application allows identifying the people who have

been in contact with someone infected with COVID-19 and tell them

of the measures that should be adopted later, such as submitting to an auto

quarantine or to the corresponding tests.

- For this, the App maintains the contacts of the people who use the app.

Application and who may have been exposed to infection of the

COVID-19.

- When a person tests positive for COVID-19 and decides to

freely share this data, the App alerts those other people who

could have been infected and with whom you have had contact

last 14 days. To do this, this person must share a number of

12 figures that will be provided by the health authorities. The mobile

performs a check if the random IDs match any

that has been marked as positive.

- The day on which the user developed compatible symptoms is determined

with COVID-19 and date of contact with infected people. The data

They may also be processed for scientific research purposes or

statistics. In this case, the data will be completely anonymised.

two.

ú A description is made of the elements involved in

each of the phases of the life cycle of the processing data

ment (activity, actors and systems).

ú A description of the intervening technologies is made.

ú Regarding legality and regulations:

Pursuant to Directive 2002/58/EC of the European Parliament and of the Con-
council, of July 12, 2002, regarding the processing of personal data
and the protection of privacy in the communications sector
electronic information (article 5), the storage of information in the
user's device or obtaining access to information and to
stored is only allowed if: i) the user has given his consent
storage, or ii) the storage or access is strictly necessary.
rios for the service of the information society, in this case the
Application, which the user has expressly requested (that is,
through installation and activation). In the case of the object Application
of evaluation, requirement ii) is not met, since the loading of data from
Proximity for contact tracing and alerting is not required for the
operation of the Application itself, therefore, it is necessary to obtain
have the free, specific, explicit and informed consent, through
clear affirmative user action.

As a legal basis for lawful processing of personal data, the
RGPD explicitly recognizes the two mentioned: mission carried out in-
public interest (art. 6.1.e) or vital interests of the interested party or other
physical ones (art. 6.1.d).

They indicate that, for the treatment of health data, it is not enough that
there is a legal basis of art. 6 GDPR, but in accordance with art.
9.1 and 9.2 RGPD there is a circumstance that lifts the prohibition of
treatment of said special category of data (among them, data of
Health). THE AEPD understands that these circumstances can be found,

in this case, in several of the epigraphs of art. 9.2 GDPR.

 Regarding the analysis of the need, proportionality of the treatment:

- Principle of purpose limitation: The main purpose of the App is

inform people who have been in close proximity to someone who

turns out to be a confirmed carrier of the virus, in order to break the chains

transmission lines as soon as possible. In this way, the Application per-

It allows identifying people who have been in contact with someone

infected by COVID-19 and inform them of the measures that are appropriate

adopt later, such as self-quarantining or being tested

corresponding diagnoses.

- Principle of data minimization: they indicate that they are collected exclusively-

the personal data required for the purposes indicated.

falls.

- Principle of limitation of the term of conservation: The terms are based

on the medical importance and on realistic timeframes for administrative measures.

which, if applicable, should be taken.

The data generated for contact tracing and alerting: The data

of proximity will be deleted as soon as they are no longer necessary

to alert people and at the latest after a period of one month

(incubation period plus margin).

The data is stored on the user's device, and only those

that have been communicated by users and that are necessary

to fulfill the purpose they are uploaded to the central validation server

of positives available to the health authorities when

chosen such an option (i.e. only the data would be uploaded to the server

of "close contacts" of a person who had tested positive for

COVID-19 infection).

In any case, personal data should only be kept during the

COVID-19 crisis. Then, as a general rule, all data

personal data should be deleted or anonymised.

• Risk reduction measures:

- The application does not collect information that is not related to the object

specific or not necessary — for example, marital status, identifiers

communications, team directory items, messages, re-

call logs, location data, device identifiers,

etc.

- The data disseminated by the applications only includes some identifiers.

unique and pseudonymous, application-generated and user-specific passwords.

is. These identifiers are renewed periodically, with a frequency

compatible with the purpose of containing the spread of the virus and sufficient

te to limit the risk of identification and physical tracking of people.

- Although the model is decentralized, a ser-

central server, of the health authority, where to register the codes of the

people diagnosed with COVID-19. This con-tracing server

tacts should be limited to collecting the history of contacts or those identified

pseudonyms of a user who has been diagnosed as infected

as a result of an adequate evaluation carried out by the authorities

sanitary and a voluntary action of the user.

- Advanced cryptographic techniques will be applied to guarantee security.

ity of the data stored in the servers and applications and the inter-

changes between the applications and the remote server. It will also proceed

to mutual authentication between the application and the server.

- Notification of users infected with SARS-CoV-2 in the application-

tion shall be subject to appropriate authorization by means of a code from a

only use linked to a pseudonymous identity of the infected person and linked

side with a screening lab or health care professional.

healthcare. If confirmation cannot be obtained safely,

No data processing will take place that presupposes the validity of the

user status.

- The data controller, in collaboration with the authorities, has

to provide clear and explicit information about the link that allows

upload the official national contact tracing app, in order to

mitigate the risk of third-party applications being used.-

under

of the principles of integrity and confidentiality, taking into account that

health data deserve higher protection, measures will be applied

appropriate up-to-date technical and organizational measures that ga-

guarantee a sufficient level of security. Such measures consist of

pseudonymization, encryption and non-disclosure agreements

as well as a strict distribution of access roles and status.

establishment of restrictions and access logs. Also, you have to

take into account national provisions that may establish requirements

specific technical specifications or other guarantees, such as the observance of the

professional secrecy rules.

Risk assessment and safeguards

The risk assessment carried out for the “Radar COVID” service is

It is included in the “Covid Radar Service Risk Analysis”,

generated with the tool "***HERRAMIENTA.1" through which the

has carried out the evaluation of risks and safeguards for the treatment

“Radar COVID” training and all the infrastructure that has been implemented

for this service.

 Action Plan:

For the COVID Radar Service, it is proposed in the AARR Report,

Take a series of necessary actions to minimize the residual risk

so that there is no asset with MEDIUM level risk. for

For this reason, those risks that are above the

value {2} and, on them, the safeguards that

were below the value recommended by ***TOOL-

TA.1 for the National Security Scheme to raise them to the re-

recommended.

 Conclusions contained in the EIPD report:

A series of actions and recommendations have been proposed in the Report

me of AARR whose implementation would mean that none of the assets

would reach a medium risk, but all could be classified as risk

low and even many of them of negligible risk.

Regarding interoperability:

1.30.- On June 16, 2020, it is adopted by consensus of the working group of the eHealth Network the document “eHealth Network Guidelines for EU Member States and the European Commission on specifications of interoperability for cross-border transmission chains between applications are approved. Detailed elements of interoperability between solutions based on COVID + keys”, in which a definitive architecture is proposed to implement the Federation Gateway service. The Federation Ga service teway, accepts diagnostic keys from all countries, stores them temporarily and provides them for download in all countries. Ade- more, all backends can be informed immediately if there are new ones data available, so that transmission delays are kept to a minimum.

cheers

On July 16, 2020, the Execution Decision was published in the DOUE (EU) 2020/1023 of the Commission of July 15, 2020 that modifies the Decision Execution Order (EU) 2019/1765 regarding the cross-border exchange data exchange between national mobile contact tracing applications cough and warning to combat the COVID-19 pandemic. This Decision is- lays down provisions on the role of participating Member States and of the Commission in relation to the operation of the federative gateway

for cross-border interoperability of national mobile applications

contact tracing and warning.

On September 2, 2020, it is adopted by consensus of the working group

of eHealth Network the document “European Certificate of interoperability.

Governance. Security architecture for monitoring and warning

of contacts applications” that establishes that the safe and trustful exchange

ble of diagnostic keys between European countries is carried out by the Euro-

pean Federation Gateway Service (EFGS) that distributes data between

member states. This exchange of diagnostic keys is secured

by cryptography transparent signatures for all countries participating in the

system. Digital signatures can be used to achieve integrity and authentication.

tenticity of the data. A well-defined confidence model is necessary

to link the public key of an entity to its identity in order to allow

other participants to verify the origin of the data or the identity of the participant.

speaker. In the context of the EFGS this means that the public keys of

European Member States also since the public key of the EFGS

must be linked to their identities to establish trust between

participants. In this way, Member States can verify the integrity

ity and authenticity of the signed diagnostic keys provided by the

EFGS. This document establishes the trust and security services that

will be established in the EFGS.

1.31.- On October 15, 2020, the SGAD contributes to the damage inspection

a copy of the Declaration and letter of intent on the connection of SPAIN

with the EFGS sent by the Secretary General of Digital Administration to the

European Commission, as well as a copy of the mandatory application form for

intention to participate in the EFGS and annexes (survey and check list).

They state that the entry into service of interoperability with Radar CO-

VID is anticipated for October 30, 2020.

2.- On December 16, 2020, information was requested from the General Secretariat

Directorate of Digital Health, Information and Innovation of the National Health System

(SGSDII), regarding the instructions given to the person in charge of the treatment, and in

particular in relation to the protection of data from the design and by default of

the "RADAR COVID" app and copies, where appropriate, of the reports prepared by the De-

Legacy of Data Protection, and in particular those related to the supervision of

treatments and the need to prepare an impact assessment related to

data protection, as well as the measures carried out by the SGSDII in

based on points 3 of the second and third clauses of the Agreement, taking into account

dated January 28, 2021, a response brief in which they report, among

others, from the following:

The Ministry of Health exercises the role of data controller through

of the General Secretariat of Digital Health, Innovation and Information of the SNS

(SGSDII), and the General Secretariat of Digital Administration (hereinafter,

SGAD), dependent on the Secretary of State for Digitization and Intelligence

Artificial (hereinafter, SEDIA), of the Ministry of Economic Affairs and Trans-

Digital Training, exercises the role of data processor from the signing of the

Agreement signed between both ministries between the Ministry of Economic Affairs

and Digital Transformation and the Ministry of Health about the application

tion "RADAR COVID", published in the BOE of 10/15/2020.

They report on the requests for reports and statistics made by

from the SGSDII to the SGAD since August 2020 and the follow-up carried out.

Regarding the evaluation of the impact of the treatments carried out by the Ra-

give COVID, they report that on December 15, 2020 a review of the

EIPD for EFGS, suggesting the performance of a penetration test and/or a

wider external cybersecurity audit after revision of the document of

risk analysis and impact analysis submitted by the person in charge of processing

I lie.

Regarding the GOOGLE app:

3.- The following checks have been carried out on a mobile device with

Android version 10.0 operating theme:

3.1.- It has been verified that the operating system has installed a new service

cio called "Notifications of exposure to COVID 19" version

17203704005. After accessing this service, the following is verified:

-

Reports the exposure checks that have been carried out in the

last 14 days (day and time).

- It has an option that allows you to eliminate random identifiers.

-

Informs that the date, duration and intensity of the event are shared with the app.

the signal associated with the exposure.

It reports on how it works and how to use the exhibition system.

Reports that the exposure system does not use, save or share the location

cation of the device and that it is necessary to activate the location of the device

because exposure notification technology uses search

of Bluetooth devices to know which ones are nearby since in all

-

-

phones running Android 6.0 and above, in order to use that

Bluetooth search, location settings must be activated

of the device for all applications, not just those that use the

exposure notification system.

3.2.- Version 1.0 of the “Radar COVID” app (pilot version) was uploaded to the re-

Google Play repository on August 7, 2020, subsequently they have been published

successive updates (from 1.0.1 to 1.0.7) until the version

1.1 (at the date of the checks carried out by the data inspection) that

was updated on October 29, 2020, in which the following have been made

checks:

- In the GOOGLE application repository it is stated that the app to date

of the report has been downloaded by more than a million users and includes

a link to the privacy policy.

- Reports the following permissions requested by the App:

either

either

either

either

either

either

either

Run service in the foreground

Access the entire network

See network connections

Request permission to ignore battery optimizations.

Prevent the phone from going to sleep

Pair with bluetooth devices

Run at startup.

After installing the application, you access it, verifying the following:

ú The app does not require registration as a user, nor does it request personal data

staff. The only information requested is the language.

ú Informs about the functionalities of the application, which works without revealing the

identity of the user or the device. Does not collect name, phone or geo-

location and that at any time you can stop using it.

ú Includes a link to the privacy policy, which must be accepted to con-

continue Include a link to the terms of use.

ú Request permission to activate COVID exposure by activating

bluetooth and to ignore battery optimization and keep running.

running in the background of the app.

ú After the installation is complete, a window with information is displayed.

on risk contacts had and with two buttons, one to activate and

deactivate the app and another to communicate a positive COVID-19.

ú By pressing the button to communicate a positive, the app requests the date of

onset of symptoms or date of sample collection or, if unknown,

ce leave it blank and a 12-digit code and informs that the informa-

tion will always be treated anonymously.

ú If the GPS antenna of the terminal (geolocation) is deactivated, the system

operative launches the following notification: “inactive exposure notification”

goes. To use this function activate the location”

Regarding the APPLE App

4.- The following checks have been made on an iPhone SE device,

with software version iOS 13.6.1.:

- In the previous update, iOS 13.5.1 and due to the expansion of the

COVID-19, APIs have been incorporated aimed at trying to stop the spread

gation that taking advantage of the functionalities of the phone at connection level

bluetooth tivity.

- In the version history there are versions from 1.0 to

1.08.

- The "RADAR COVID" app has been installed on the device.

vo, performing the following checks:

o The app does not require user registration, nor does it request character data.

be personal.

o Informs that the application works without revealing the identity of the user.

river, and that at any time you can stop using it.

o Includes a link to the privacy policy, having to accept it to

continue. Include a link to the terms of use.

o Request permission to activate exposure to COVID by activating

Bluetooth connection and to receive notifications.

o Once the installation is complete, a window with two buttons is displayed.

tions, one to activate and deactivate the app and another to communicate a possi-

tive COVID-19.

o By pressing the button to communicate a positive, the app requests the date of

onset of symptoms or date of sample collection or, if unknown,

noce leave it blank and a 12-digit code and informs that the in-

training will always be treated anonymously.

o At no time is activation of the location service requested.

Regarding the DP-3T protocol on which RADAR COVID 19 is based:

5.- DP-3T is a collaboration of researchers from all over Europe who joined forces

strengths to create an open technical solution to proximity tracking for epide-

mia COVID-19 respecting personal privacy. They have designed and developed

we developed proximity tracking systems with the aim of preserving privacy

dad.

DP-3T has made public technical documentation of this protocol in the repository

https://github.com/DP-3T/documents, which is also provided by the inspector

nate as the basis of the developments of the RADAR COVID 19 system, and of the analysis

of this, the following relevant points stand out:

- The document “Decentralized Privacy-Preserving. Proximity Tracing .Overview

of Data Protection and Security” shows that in this system,

centralized there are five main actors relevant to data protection:

ts: users, health authorities, a back-end server, research projects

epidemiological investigation and providers of mobile telephony operating systems.

vile (in this case, Apple and Google). Apple and Google only provide a service

push notification service, the same as for any application and are con-

aware that the application has been installed, acting as processors,

but they cannot see any content or data. The same document states

since Apple and Google provide the operating system

manifest that "

running on mobile devices, one has to trust them, since

could potentially become aware of information related to the

proximity tracking system (who is infected, who infected whom,

social graphs, etc.)".

In addition, the document states that "the system is designed in such a way

that no entity beyond a user's device processes or stores

personally identifiable data about the user. As a whole, the system

meets treatment goals that would normally require transmission

sion of personal data. We believe that, within the framework of the normal functioning

wrong, none of the data used to achieve proximity tracking should be

be characterized as personal data, since no actor who owns the data

has the ability to re-identify them with reasonably sustainable means.

capable of being used."

As for the identifiers, mobile phones with the security application

installed proximity tracking emit ephemeral bluetooth identifiers

(EfIDs) via Bluetooth Low Energy. These ephemeral identifiers

are pseudo-randomly generated by the phone, derived from the key se-

crete SK of the phone itself.

- The document “Best Practices Operational Security for Proximity Tracing” des-

Create security mechanisms that can be added to security applications.

proximity tracking to ensure that security properties and

privacy provided by the protocols are not undermined by other

System Components. The following can be deduced from this document:

“There are two types of requests to the server: non-sensitive requests

and confidential. In decentralized proximity tracking systems

two, all users regularly retrieve new diagnostic keys

and potentially new app configurations. These requests do not

they are sensitive. All users make these requests, and therefore

their records may not reveal any confidential information about

users, beyond the fact that these users use an application

proximity tracking. Requests made by users related to

related to the loading of diagnostic keys by users positi-

vos COVID-19 and requests to confirm the notification status of the

exposed users are sensitive. These requests should be treated with

watch out. “

The document highlights communications as a vulnerable point in the system.

that are established between devices and servers, which include

metadata.

The document proposes that applications program false actions. East

protection mechanism works by (1) producing false actions

actions that are indistinguishable from real actions and (2) the distribution of these

false actions over time. As a result, any observed action

vada could, with a reasonable probability, be a false action.

The document “Privacy and Security Risk Evaluation of Digital Proximity Tracing

Systems”, also in reference to the traffic of data on infected patients

stresses that “Any proximity tracking system in which people

infected people upload data directly from your phone to a central server.

unmeasured, reveals to a potential network observer that a patient su-

uploaded data to the central server.

Most proposals for proximity tracking systems

assume that shortly after an application user receives a result,

positive state of the test, it will load the necessary information to trigger

Send contact tracing from your personal device to a server

central. This allows a spy connected to the network, for example, a curious

internet service provider, wifi provider, would you know that this is

an infected user. It also allows the central server to obtain a pseudo-

teething for the infected person.

A proxy does not help mitigate this attack. Users can upload regular-

mind dummy packets, for example, empty messages of the same size as

a real report, to the server. The server will simply ignore these packets

fictitious. Since users use an encrypted connection to the server,

network observers cannot distinguish these dummy packets from the

actual loads, thus hiding their infection status even from observers.

res of the network.”

This vulnerability was corrected in the Radar COVID app and uploaded to the Gi-

thub on October 8, for the following versions of the application: Android,

version 1.0.7, Apple, version 1.0.8

Regarding the Apple and Google APIs:

6.- Technical documentation of this interface has been made public on different websites

of Apple and Google, which has also been provided by the inspected as

basis of the developments of the RADAR COVID 19 system, and its analysis,

The following relevant points stand out:

- The “Exposure Notification Bluetooth Specification” document provides the

Detailed technical specification for a new Bluetooth protocol that preserves the

privacy to support exposure notification. Highlight as a requirement is-

essential in the design of this specification to maintain the privacy of users.

rivers by the following means:

either

either

either

either

The Exposure Notification Bluetooth specification does not use the

location for proximity detection. Use strictly beacon-

Bluetooth ment for proximity detection.

A user's proximity identifier changes on average every

15 minutes and you need the temporary exposure key to map-

tion with a contact. This behavior reduces the risk of loss

gives privacy by the dissemination of identifiers.

Proximity identifiers obtained from other devices are

processed exclusively on the device.

Users decide whether to contribute to the exposure notification.

either

If diagnosed with COVID-19, users must provide their

consent to share diagnostic keys with the server.

Users have transparency in their participation in the notification

of exposition.

- The document “Exposure Notification Cryptography Specification” provides the

Detailed technical specification for the encryption of the new Bluetooth protocol. It is-

specifies the following privacy considerations:

either

either

either

either

The programming of keys is fixed and defined by the components of the

operating system, which prevents applications from including information

static or predictable information that could be used for monitoring.

A temporary exposure key is required to correlate between

the changing proximity identifiers of a user. This reduces

increases the risk of loss of privacy due to the dissemination of the identified

beef.

Without the publication of temporary exhibition keys, it is compu-

infeasible for an attacker to find a match/co-

response in a proximity identifier. This avoids a wide

range of replay and spoofing attacks.

When reporting diagnostic keys, the correlation of the identified

Proximity resers by others is limited to 24-hour periods due to the

use of temporary exposure keys that change daily. The

server should not keep metadata of uploading users

diagnostic keys after including those keys in the added list.

gada of diagnostic keys per day.

7.- Other relevant considerations:

Report of the School of Computer Science & Statistics, Trinity College.

7.1.- In July 2020 the university center “School of Computer Science &

Statistics, Trinity College. Dublin” published a report analyzing

the actual data transmitted to the back-end servers by the applications of

contact tracing implemented in Germany, Italy, Switzerland, Austria,

Denmark, Spain, Poland, Latvia and Ireland, as well as the data

transmitted by the APIs of GOOGLE and APPLE, in order to evaluate the

user privacy.

Concludes the Trinity College report that analyzed the data transmitted to

back-end servers by contact tracing apps

implemented in said countries in order to evaluate the privacy of the

Users consist of two separate components: a "client" application

administered by the national public health authority and the health service

Google/Apple exposure notification, which on Android devices is

managed by Google and is part of Google Play Services. The

health authority client applications generally behave well

from the point of view of privacy. However, the component of

Google Play Services of these applications is worrying from a point

privacy view. Google Play Services contacts users

Google servers approximately every 20 minutes, which allows

potentially location tracking with accurate products through

of the IP address. In addition, Google Play services also share the

Phone IMEI, hardware serial number, SIM serial number,

phone number of the user's phone and email address

with Google, along with detailed data on the applications running

on the phone. This data collection is enabled simply by enabling

Google Play services, even when all other services and

Google settings are disabled.

On the occasion of this report, the Irish Control Authority has questioned

GOOGLE the issue of personal data processing in the context

of the use of the API, whose response has been shared with all

authorities through IMI (Informal Consultation 141776).

In the response given, Google alleges the following:

“The metrics and telemetry covered in this report describe a

industry practice for mobile operating systems (not just in

Android) that helps ensure devices stay up to date.

updated, keep people and systems safe from hacks.

ques and enable reliable operation of the device ecosystem

androids. As explained later, there is no connection between the

general remarks about Android telemetry in the report and

the use of exposure notification applications. although always

We are open to working with the research community to improve

general standards for Android, we are disappointed with the way

that researchers have tried to confuse the general telemetry of

Android with the exposure notifications APIs.

The Android Device Configuration Service periodically sends-

Mind data from Android devices to Google. These data help

Google to ensure that the device is up to date and working as

best possible". In order to ensure the continuous operation of

Android devices, this system processes device identifiers

devices and accounts, device attributes, software versions, and

security firmware, network connectivity, and performance data. The

The purposes of this processing include helping to ensure that the

device receives software updates and security patches,

make applications and services work consistently across

a wide variety of Android devices with different specifications

tions and software, protect the Android device and system against

fraud, abuse and other harmful behavior, maintain metrics

Added on Android devices.

There is no connection between the general observations on telemetry

Android and Android Configuration Service report

research and use of exposure notification applications, ex-

I accept the use of an Android device for any purpose means

necessarily certain information is necessary to operate the device.

vo. In accordance with our privacy commitments for APIs

exposure notification, Apple and Google do not receive information

about the end user, location data or information about any

any other device that the user has been near.

Apart from the Android device configuration service, the data

very limited and anonymous diagnostic data are collected from the APIs of non-

exposure certifications and this has been made transparent. For example,

Google has published the specifications on the site for develop-

Android res. For its part, Google does this in order to verify

that the basic functionality (i.e., the notification mechanism of

exposure) is working and to provide a warning signal

early to investigate specific device models in case

of any problem.

By design, no user-identifying information is recorded.

user of the exposure notification system nor in its functioning

or the limited diagnostic data collected from it. Men-

unidentified log messages, received in aggregate batches, which

they only indicate information about the operation of the system, such as whether the

BLE functionality works. This registration system also interrupts

eg explicitly any links between the log messages of the

same device. Additionally, identifiers such as IP addresses

required to deliver the log message are not logged in the

disk of this log pipe.

Until now, diagnostic information has helped identify

early problems in exposure notification implementations

sation all over the world. For example, it helped identify models of

Devices that did not support the initial version of email notifications

exhibition and to develop works to guarantee a wide availability

ity. Without this information, we would not have been able to have an answer

quickly and forcefully to this urgent global pandemic."

7.2.- On September 9, 2020, the Secretary of State for Digitization

and Artificial Intelligence published the source code of the App in the repository Gi-

thub.com, in which it was possible to observe that in lines 198-199 there appears a

comment recommending the use of the Firebase development library for

Google Analytics. In response to the requirement of the Data Inspection to

In this regard, the representative of the General Secretariat of Di-

gital provides a report that highlights the following:

"Google's Firebase software libraries were used in the

pilot phase as a result of the ANR incident report (application

tion is not responding) on mobile devices, about incidents not re-

ported or bugs that are not visible to the user, but can

affect the proper functioning of the application.

…

This functionality has only been used in the pilot phase, not being in

use in the production versions currently as can be seen in

the analysis of the source code published in the github repository."

7.3.- On September 30, 2020, an email entered the AEPD

email signed by 11 teachers from different universities communicating

a vulnerability of the RADAR COVID app (...). The mail includes a report

technical and legal assessment.

According to said report, only COVID positive users upload the keys

TEK keys with the result of a test to the radar server-covid-backenddp3t-

server. Therefore, every time a key upload is observed from a

phone to this server, it can be inferred that the owner of the phone is CO-

VID-positive. The encryption between the application and the server does not help to find

open that information: even if the endpoint and content of the upload are not

observable, the length of the messages will reveal an upload of the key TEK

to the server. Communication can be observed by various entities. By

example, the telecommunications provider (if the connection is made through

of GSM); the Internet service provider if the connection is made through

from Internet; or anyone with access to the same network (WiFi or Ethernet)

than the user. In the case of the Radar COVID app, in which uploads are

they do using the Cloudfront endpoint that is used for downloading

TEKs, Amazon also has the ability to look at the addresses

IP addresses of Radar COVID users and associate them with the fact that those

users report a positive COVID test. But apart from the fact

communicate the IP address, taking into account that, as shown in the information

technical me, only COVID positive users upload the keys to the server

radar-covid-backend-dp3t-server, that IP is associated with the cla-

TEK times uploaded, which always correspond to the communication of a possible test.

COVID-positive. In this way, the operation of the app allows linking

unequivocally an IP with the fact that its holder is uploading a

positive COVID test.

On October 2, 2020, the data inspection requests information from the

regarding SEDIA and dated October 7 and 27, 2020 they have entry

two separate written responses in which the following is made clear:

This vulnerability was already known to the Radar development team.

give COVID, since it appeared in at least one technical document published

Done in April 2020 by the DP-3T team: Privacy and Security Risk Eva-

location of Digital Proximity Tracing Systems.

However, the development team did not consider it necessary to solve

this problem in the first versions of Radar COVID since,

To exploit this vulnerability, a remote scene must be assumed.

where the telecommunications operator is interested in obtaining

obtain this clinical information from their clients by studying the traffic of damage

cough generated by Radar COVID apps.

Number of identifiers that have been affected by the vulnerability

dad:

The Radar COVID app was launched nationally on 19th

August 2020.

The vulnerability was corrected in the upload corresponding to October 8.

tube, for the following versions of the application: Android, version

1.0.7, Apple, version 1.0.8.

As of October 8, a total of 3,059 codes had been declared

at the national level.

Actions taken for its resolution:

The code of the Radar COVID system was published openly on 9

September 2020, for general knowledge, which has allowed

that numerous experts in development, privacy, data protection

and cybersecurity could have access to it.

As a result of this publication and its subsequent analysis, a series of experts

in privacy they contacted the support team of Ra-

give COVID in mid-September to report on the vulnerability

ity previously described. This vulnerability has been documented

by the DP-3T team as NR-2 (traffic analysis reveals data about in-

fected patients) in their report “Privacy and Security Risk Evaluation of

Digital Proximity Tracing Systems”.

The solution to the problem, already documented in the mentioned document,

is that all Radar COVID applications generate traffic

random with the same pattern of interaction with the server (size of

packets, send/response flow, and processing times) that the

positive statements. In this way, the tra-

fico real of the simulated.

Upon learning of this vulnerability, the Radar team

COVID implemented an algorithm whereby all applications

they periodically send fictitious data frames (fake frames).

These frames are indistinguishable from real frames, both in volume

information transmitted: padding is done with fake keys until comp-

complete frames with 30 keys in total; as in processing time

on the server: since the processing time of the fake frames in

server would be lower because they are discarded without storing in the BBDD,

includes an artificial wait until completing 2 seconds of processing.

server, which corresponds to the average processing time

thinking of real positives.

The dummy traffic is implemented using a dummy function on the devices.

mobile positives, both Android and iOS. In the same way, it is im-

complements a complementary functionality in the backend, identifying

those false frames that have been generated and discarding their content.

do.

The randomness of these communications has been implemented initially

following a uniform distribution, forwarding frames with an in-

average interval around 3 hours.

Subsequently, the DP-3T team has suggested that the fake traffic is

subject to an exponential function, with an average of one remission

every five days, which introduces random time latencies between

different generated frames, which make the traffic virtually

impossible to distinguish from actual shipments.

An exchange of emails and a videoconference have been held in-

between the Radar COVID team and the DP-3T team throughout the month of October.

tuber, and finally the proposal to change the uniform distribution was accepted.

form an exponential distribution. This change will be incorporated into

a new version of the system that is expected to be released on Friday

on October 30, 2020, along with other features.

Regarding the use by third parties of the exposed data:

They state that the Radar COVID team is not aware of any use

lization by third parties of the exposed data.

It has been verified by data inspection that version 1.0.7 of the Ra-

give COVID uploaded to Google play on October 8, 2020 reports, among the non-

truths, the inclusion of sending false positive communications. It has been verified

verified that version 1.1.0 has been uploaded to the Google repository on the 29th of

October 2020.

It has also been verified that the publication of the software components

has been updated several times at https://github.com/radarcovid at

several dates from November 8 and 4, 2020."

EIGHTH: On May 21, 2021, the director of the AEPD agreed to initiate

sanctioning procedure to the GENERAL DIRECTORATE OF PUBLIC HEALTH (in what

hereafter, DGSP), in accordance with the provisions of articles 63 and 64 of the Law

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

Public Actions (hereinafter, LPACAP), for alleged violation of the following

GDPR articles: 5.1.a); 5.2; 12; 13; 25; 28.1 and 28.3; and 35, typified in the

articles 83.4.a) and 83.5.a) and b) of the RGPD.

NINTH: On June 2, 2021, the DGSP submits a document through the

which requests the extension of the term to submit allegations and provide documents or

other judgment elements.

TENTH: On June 2, 2021, the examining body agrees to extend the

period requested up to a maximum of five days, in accordance with the provisions of article

32.1 of the LPACAP.

The extension agreement is notified on June 3, 2021, through the Service

of Electronic Notifications and Authorized Electronic Address.

ELEVEN: On June 11, 2021, the DGSP submits a document through the

requesting a new period to submit allegations and provide documents or other

elements of justice.

The denial agreement is notified on June 14, 2021, through the Service

cio of Electronic Notifications and Authorized Electronic Address.

TWELFTH: On June 11, 2021, having notified the aforementioned start-up agreement, the

DGSP presented a brief of allegations in which, in summary, it stated that:

FIRST.- Work overload due to the pandemic:

Since the declaration of the State of Alarm on March 14, 2020, this Directorate

tion General has seen its workload increased to levels that have

come to jeopardize its operation.

You have found yourself in a defenseless situation during the action phase.

previous instructions, since no requirements have been made to this management center

nor to the Secretary of State for Health so that the evidence could be provided

and necessary justifications that, if applicable, proceed.

On the contrary, the AEPD did ask the SEDIA and the SGSDII for a request

of information on December 4, 2020.

SECOND.- Situation prior to the October 13 Agreement.

The regulations referred to in the RADAR Privacy Policy

COVID (specifically, the Ministerial Order SND/297/2020 of March 27) effective

entrusts SEDIA with the development of new actions for the

management of the health crisis caused by COVID-19.

The Ministerial Order of March 27 determines that the data controller

This will be the Ministry of Health and the person in charge of the treatment and owner of the application.

cation will be the General Secretariat of Digital Administration (hereinafter, SGAD).

In other words, it is not specified which administrative body of the Ministry of Health is

the person in charge of the treatment, if not that it is attributed to the Ministry of Health in

your set.

However, as recognized by the AEPD, it cannot be framed in this Or-

Ministerial give the RADAR COVID-19 app. The same happens with the Royal Decree-

Law 21/2020, of June 9, on urgent measures of prevention, containment and

coordination to deal with the health crisis caused by COVID-19.

The AEPD acknowledges in the agreement to initiate the procedure that SEDIA

acted as data controller from the start-up of the application.

tion until the October 13 Agreement.

THIRD.- Situation as of the Resolution of October 13.

On October 13, 2020, the Undersecretary of the Ministry of the Presidency

dence, Relations with the Courts and Democratic Memory dictates Resolution by

which publishes the Agreement between the Ministry of Economic Affairs and Trans-

Digital Training and the Ministry of Health, about the RADAR CO-

VID-19.

Said resolution is signed by the SGSDII on behalf of the Ministry of

Health, who is responsible for addressing projects of modernization, innovation,

improvement and transformation of the National Health System, as stated in its

second section. Likewise, the Resolution of October 13 points out, as

has been reported, the role played up to now by the Ministry of

Health.

“The SGAD has been developing, with the knowledge and agreement of the Ministry

Ministry of Health, an application for the traceability of contacts in relation

to the pandemic caused by COVID-19 called "Radar COVID". du-

During the month of July 2020, with the agreement of the General Directorate of

Public Health, Quality and Innovation of the Ministry of Health, the SGAD carried out

successfully carried out the pilot project of the same, whose success guarantees the viability

of the proposed solution for close contact tracing.”

Along the same lines, it is noted that:

"Until now, the Ministry of Health has been collaborating with the

SGAD, owner of the “Radar COVID” application, in the functional adjustment processes

of the same from the perspective of public health, coordinating the protocols

the epidemiological management of cases detected through the application, and

favoring the progressive incorporation of autonomous communities and cities

more to its use in the testing phase with real data according to the aforementioned

Agreement of August 19, 2020."

Once again, the aforementioned Resolution of October 13 includes the paper that until now

time the Ministry of Health had performed in relation to RADAR

COVID-19: that of "collaborating" with the Ministry of Economic Affairs and Transformation

Digital information, "coordinate" epidemiological management protocols and "favor"

that the Autonomous Communities and autonomous cities signed collaboration agreements

for its effective implementation throughout the national territory.

In the operative part of the aforementioned Resolution of October 13, both parties

agree to delegate to the SGAD all the powers of design, development, im-

planting and evolution of the RADAR COVID-19 application, as well as the capacity

ability to sign inter-administrative agreements with the Autonomous Communities and cities

plus.

Finally, the second clause, section 3, specifies that:

"In relation to the delegation of powers provided for in letter b) of the clause

first clause of this Agreement, correspond to the General Secretariat of Health

Digital, Information and Innovation of the National Health System, in its condition

Responsible for the processing of personal data, give the indications

necessary to the SGAD in its capacity as data processor."

From what is stated in the aforementioned resolution, a new distribution of roles in

in relation to the treatment of the information collected by RADAR COVID-19: for

On the one hand, the SGSDII begins to play the role of data controller;

on the other, the SGAD would be in charge of the treatment.

It should be noted that the clauses of the aforementioned Resolution of October 13 in

At no time does it refer to the General Directorate of Public Health.

Finally, as stated in the resolution of the AEPD of May 21, it is

makes it necessary to indicate that, at the request of the AEPD, the SGSDII reaffirmed the

content of the Resolution of October 13, assuming the role of responsible

of the treatment.

FOURTH.- Legal basis

One: SEDIA acted as controller of the information collected.

confirmed by RADAR COVID-19 until formalization, by means of a Resolution with

Date of October 13, 2020, of the Agreement between the Ministry of Economic Affairs

micos and Digital Transformation and the Ministry of Health.

Two: The Ministry of Health plays, through the SGSDII, the role of res-

responsible for the treatment of information since October 13, 2020, in

under said Agreement.

Three: In no resolution, agreement or legal act is the General Management

General Public Health as responsible for the treatment of general information

Rated by the RADAR COVID-19 app.

As the AEPD points out, the General Directorate of Public Health is responsible for

among other functions, and in accordance with article 4 of the Royal Decree

735/2020, of August 4, which develops the basic organic structure

of the Ministry of Health, and modifies Royal Decree 139/2020, of January 28,

ro, which establishes the basic organic structure of the departments

ministerial, the coordination of surveillance in public health. Specifically, and
for the case at hand, section 7, letter e), states that the DGSP will exercise
the function of: Monitoring risks to public health in coordination with
the bodies involved and carry out the appropriate risk assessments.
As is evident, the attribution of this function finds its foundation in the
current legislation on health matters, namely, Organic Law 3/1986, of 14
of April, of Special Measures in the Matter of Public Health or Law 33/2011,
of October 4, General of Public Health, in addition to other regulations of a nature
regulatory. However, the attribution of such functions does not imply that this
General Management has to assume, automatically and unequivocally, the role of
responsible for processing the information collected by RADAR COVID-19.
As stated in the Resolution that agrees to start the procedure
sanctioning party, before the Agreement of October 13, 2020, the Director General
of Public Health sent a letter to SEDIA in which, on the one hand, the
approval for the development of the pilot test of the mobile application and,
another, it was transferred that, to the good understanding of this General Directorate, the
responsible for the processing of personal data would be the health authorities
of each of the Autonomous Communities.
This interpretation was based, as has been reported, both on the role that until now
time had assumed the General Directorate of Public Health as in the district
competence determination determined in current regulations. So the article
149.1.16ª of the Spanish Constitution attributes to the State the bases and coordination
general health policy, leaving the development and implementation of health policy
ria corresponds to the Autonomous Communities. This distribution of competence
cias is delimited and reinforced by current regulations, including the Law
14/1986, of April 25, General Health, where, at the time of distributing the com-

competitions between the different Administrations, it is contemplated that the establishment

development of media and relationship systems that guarantee information and co-

reciprocal communication between the State Health Administration and that of the

Autonomous Communities will be developed by the State "without detriment to the

competences of the Autonomous Communities", as stated in the article

article 40.16 of the aforementioned regulation.

Along the same lines, both the General Health Law and the legal regulations and regulations

subsequently approved regulation determines that the services of the System

National Health correspond, practically in its entirety, to the administrations

of the Autonomous Communities. Without prejudice to the coordination functions

attributed to the Ministry of Health, such is the case of services related to the

training and epidemiological surveillance, in accordance with the provisions of Annex I

of Royal Decree 1030/2006, of September 15, which establishes the charge

tera of common services of the National Health System and the procedure

for your update.

Consequently, the General Directorate of Public Health, in good faith and attending

complying with the aforementioned regulations, understood that the responsibility for the treatment

I would ponder the regional authorities, since they are the ones competent to

health care of the population and, therefore, have the information systems

health matics and individualized clinical data on which the mea- sures are based.

epidemiological data of a state nature. All this, at a time when this

General Directorate suffered an extraordinary workload caused by the following

situation of health emergency derived from the pandemic.

Thus, and by virtue of Royal Decree 735/2020, of August 4, the Ministry of Health

entity directs its interventions in public health under the principle of unity

capacity of action, so that the management centers that comprise them contribute

refer to the main function of the Department, which is none other than “the proposal and

implementation of the Government's policy on health, planning and assistance

health care, as well as the exercise of the powers of the Administration

General of the State to ensure citizens the right to protection of

health".

As stated in the resolution of May 21 of the AEPD, the expository part of the

Royal Decree 735/2020, of August 4, determines that:

By means of this royal decree, the structure of the

Ministry of Health, contemplating the creation of the General Secretariat of

Digital Health, Information and Innovation of the National Health System, of which

The General Directorate of Digital Health and Information Systems will depend on

the National Health System, with the aim of addressing the projects of mo-

dernization, improvement and transformation of the National Health System, in light of

the new challenges arising from the pandemic caused by COVID-19, and in

particularly those related to digital health, interoperability and services

networked at the national, European and international levels, as well as the

health information, promoting the incorporation of the benefits of the

state-of-the-art emerging technologies such as data analytics

("big data"), artificial intelligence or predictive analytics, among others, in the

health field.

Likewise, the literal tenor of article 7.1 of Royal Decree 735/2020, of 4

August, declares that:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

58/168

The General Secretariat of Digital Health, Information and Innovation of the System
National Health is the governing body of the Department to which it corresponds
address modernization, innovation, improvement and transformation projects
of the National Health System in light of the new challenges arising from the pan-
COVID-19 pandemic, particularly those related to digital health and systems
information topics. Likewise, it is responsible for carrying out activities
aimed at transferring innovation and advances in research to the System
ma Nacional de Salud, without prejudice to the powers attributed to the Ministry
Science and Innovation and the autonomous communities. Furthermore, article 8
of the aforementioned rule determines that it corresponds to the General Directorate of
Digital Health and Information Systems for the National Health System,
as a body attached to the aforementioned General Secretariat.

In addition, article 8 of the aforementioned rule determines that it corresponds to the Di-
General Directorate of Digital Health and Information Systems for the National System
Ministry of Health, as a body attached to the aforementioned General Secretariat
The development of digital public services, the promotion of digital health and the
electronic interoperability of clinical and health information, both in the field
both nationally and internationally, as well as innovation in data analytics
data and exploitation of health-related information.

In light of the foregoing, it can be concluded that although the General Directorate of

Public Health performs functions directly related to the purposes of the

RADAR COVID application, it cannot be affirmed that it is the only directing center

of the Ministry of Health that holds that character. Quite the contrary, other centers

directors, such as the SGSDII, have powers directly attributed to them

related to the determination of the purposes and means in the treatment of the

information collected by RADAR COVID-19, being able to assume, within the framework

national and European regulatory framework, the role of data controllers, as

as stated in the Resolution of October 13 between the Ministry of Ecological Affairs

Economics and Digital Transformation and the Ministry of Health.

FIFTH.- Commitment to the regulations on data protection of

personal character.

The General Directorate of Public Health has always tried to guarantee

compliance with current regulations on personal data protection.

personal nature, despite the high workload that it entails, even today

today, the health emergency caused by the COVID-19 pandemic for

this management center.

REQUESTS That the sanction proposal be dismissed, filing the procedure

I'm lying.

These allegations have already been answered in the motion for a resolution and are reiterated,

in part, in the Legal Basis of this Resolution.

THIRTEENTH: On September 22, 2021, the instructor of the procedure

agreement agrees to open a trial period addressed to the DGSP in the following

you terms:

1. Claims filed by

an ANONYMOUS PERSON, A.A.A., B.B.B. and RIGHTS INTERNATIONAL SPAIN, and

the accompanying documentation.

2. The documents obtained and generated by the Inspection Services before the

SECRETARY OF STATE FOR DIGITALIZATION AND ARTIFICIAL INTELLIGENCE

(SEDIA) and the GENERAL DIRECTORATE OF PUBLIC HEALTH (DGSP), and the Report

of previous actions of the General Subdirectorate of Data Inspection that

They are part of file E/03936/2020.

3. Likewise, the allegations to the

initiation agreement PS/00233/2021 presented by the DGSP, on the 11th of

June 2021, through the Registry of the D.G. OF PUBLIC HEALTH, QUALITY AND

INNOVATION.

4. The DGSP is REQUIRED to provide the following information and/or documentation-

following:

4.1. Regarding the Radar COVID PILOT APPLICATION launched in-

between June 29 and July 29, 2020 on the island of La Gomera and from 18

August 2020 nationwide:

b)

a) Documentation accrediting the participation of the Ministry of Health.

(through the corresponding superior or managerial body) in the development

Development and launch of the pilot project.

Information on the data collected through the pilot application (in-

including connection data between the user's terminal and the server and

the metadata).

Information on the processing of personal data -understood as the

set of operations carried out on these data - by the Ministry

Health Department or other higher or managerial body of the department.

Information on the following question: What did the material materially consist of?

that data processing?

Specifically, the life cycle of the data processed, the process of these

from its collection to its deletion or blocking.

d)

c)

e) In the information related to the pilot project on the island of La Go-

reference is first made to the fact that it is an experience with fictitious data.

Whoa. And it is added that: “the data handled by the application does not allow

the direct identification of the user or his device (...)”.

In view of these references, the DGSP is required to report

about whether he was aware that data processing would be carried out

in the pilot project and, in any case, from the moment in which

was aware of these treatments.

f) Copy of the record of personal data processing activities

made in the pilot project. Said register, referred to in article

30 of Regulation (EU) 2016/679, of April 27, 2016, must

be provided in its initial version, together with any additions, modifications or

exclusion in the content of this.

g) Copy of the impact assessment related to the protection of data res-
regarding the pilot project and documentation related to it. Specification
of the subject that elaborates it and the moment in which it is carried out (start date
and completion).

h) If the impact assessment was prepared, supporting documentation of the
participation of the data protection delegate of the Ministry of Health
give in this
Analysis of data protection risks on the pilot project and do-
documentation related to this. Specification of the subject that prepares it and the
moment in which it is carried out (start and end date).

Yo)

j) Copy of the content of the minutes of the meetings held between the Di-
General Directorate of Public Health, Quality and Innovation, or another body
superior or director of the Ministry of Health and SEDIA, which include the
information regarding agreed decisions on protection
of data applicable to the pilot project, with identification of the condition
of the different participants (responsible or in charge).

k) Copy of the content of the minutes of the meetings held between the Mi-
Ministry of Health (or its superior or directive body), SEDIA and the
Autonomous Community of the Canary Islands, on the project for the application of
Radar COVID, which include the information related to the decisions agreed
given in terms of data protection applicable to the pilot project.

l) Copy of the content of the agreement of the Interterritorial Council of the system
national health policy adopted on August 19, 2020, on the use
of the “Radar COVID” application, in the testing phase, by the co-

autonomous communities and cities.

m) Documentation accrediting the contract or other legal act signed between the General Directorate of Public Health, Quality and Innovation or another superior or director of the Ministry of Health and SEDIA, for the implementation of the pilot project, in accordance with the provisions of article 28.3 of Regulation (EU) 2016/679, of April 27, 2016.

n) Documentation accrediting prior authorization, in writing, specifically fica or general, in favor of SEDIA or the General Secretariat of the Ad- Digital Administration (SGAD) by the General Directorate of Health Public, Quality and Innovation or another higher or directive body of the Ministry Ministry of Health, in relation to the contract signed between the SGAD and IN- DRA on June 15, 2020, in accordance with the provisions of article 28.2 of Regulation (EU) 2016/679, of April 27, 2016 -which had the purpose of contracting the services of "Design, development, pilot and evaluation of a system that allows the traceability of contacts in re- to the pandemic caused by Covid-19-.

o) Competence on the basis of which, the General Director of Public Health, Quality and Innovation, communicates the approval of the Ministry of Health for the development of the application, in the communication dated June 9 of 2020.

The previous information and documentation foreseen in section 4.1 -insisti- we- is required in relation to the pilot test, from the beginning of the actions

tions related to it, including the phase prior to its start-up

and subsequent development, until its completion.

4.2. Regarding the Radar COVID APPLICATION launched in the different

autonomous communities and cities after accession through the

appropriate bilateral agreements signed between the Ministry of Health and the

Corresponding ministries:

b)

c)

a) Personal data required by the Radar COVID application to function

operate correctly and fulfill its purposes.

Information on the processing of such personal data, understood

as the set of operations performed on that data.

Information on the following question: What has the material-

Mind that data processing?

Specifically, the life cycle of the data processed, the process of these

from its collection to its deletion or blocking.

d) Documentation accrediting whether the protection delegate has been requested

tion of data from the Ministry of Health advice on the nature

legal validity of the data processed and the response, which, where appropriate,

have formulated.

e) Documentation accrediting the documented instructions directed

SEDIA or SGAD, in accordance with the provisions of article 28.3.a) of the

Regulation (EU) 2016/679, of April 27, 2016.

f) Copy of the record of personal data processing activities

made in the Radar COVID application. Said register, to which

re Article 30 of Regulation (EU) 2016/679, of April 27, 2016,

must be provided in its initial version, together with any additions, modifications,

cation or exclusion in the content of this.

g) Impact assessment(s) relating to data protection

regarding the Radar COVID application.

The information and documentation provided for in section 4.2 is required in re-

connection with the commissioning of the Radar COVID application from the 10th of

October 2020, after the publication in the BOE of the Resolution of October 13

2020, of the Undersecretariat, by which the Agreement between the Mi-

Ministry of Economic Affairs and Digital Transformation and the Ministry of

Health, about the "Radar COVID" application.

On October 3, 2021, the notification was considered rejected after

ten calendar days from its availability, without access to its

contents.

FOURTEENTH: On September 22, 2021, the instructor of the procedure

agreement agrees to open a trial period that directs the SGSDII in the following

following terms:

The GENERAL SECRETARIAT OF DIGITAL HEALTH, INFORMATION AND

INNOVATION OF THE NATIONAL HEALTH SYSTEM (hereinafter, SGSDII), to

that provides the following information and/or documentation:

1. Regarding the Radar COVID PILOT APPLICATION launched between

on June 29 and July 29, 2020 on the island of La Gomera and from

August 2020 nationwide:

a) Documentation accrediting the participation of the SGSDII in the de-

b)

c)

d)

Development and launch of the pilot project.

Information on the data collected through the pilot application (in-

including connection data between the user's terminal and the server and

the metadata).

Information on the processing of personal data -understood as the

set of operations carried out on these data - by the

SGSDII.

Information on the following question: What did the material materially consist of?

that data processing?

Specifically, the life cycle of the data processed, the process of these

from its collection to its deletion or blocking.

e) Copy of the record of personal data processing activities

made in the pilot project. Said register, referred to in article

30 of Regulation (EU) 2016/679, of April 27, 2016, must

be provided in its initial version, together with any additions, modifications or

exclusion in the content of this.

f) Copy of the impact assessment related to the protection of data res-

regarding the pilot project and documentation related to it. Specification

of the subject that elaborates it and the moment in which it is carried out (start date

and completion).

g) If the impact assessment was prepared, supporting documentation of the

participation of the data protection delegate of the Ministry of Health

give in this

h) Analysis of data protection risks on the pilot project and do-

documentation related to this. Specification of the subject that prepares it and the

moment in which it is carried out (start and end date).

i) Copy of the content of the minutes of the meetings -in case of attendance-

ted- in which the SGSDII has participated together with the SECRETARIAT OF

STATE OF DIGITALIZATION AND ARTIFICIAL INTELLIGENCE (SEDIA),

that include the information related to the decisions agreed upon in matters

data protection legislation applicable to the pilot project, with identification

of the condition of the different participants (responsible or in charge)

two).

j) Copy of the content of the minutes of the meetings held between the

SGSDII -in case of having attended-, SEDIA and the Autonomous Community

of the Canary Islands, on the Radar COVID application project, which includes

include information relating to agreed decisions regarding

data protection applicable to the pilot project.

k) Documentation accrediting the contract or other legal act signed between

SGSDII and SEDIA, to carry out the pilot project, in accordance with

the provisions of article 28.3 of Regulation (EU) 2016/679, of 27

April 2016.

l) Documentation accrediting prior authorization, in writing, specifically

fica or general, in favor of SEDIA or the General Secretariat of the Ad-

Digital Administration (SGAD) by the SGSDII, in relation to the

contract signed between the SGAD and INDRA TECNOLOGÍAS DE LA INFOR-

MACIÓN S.L, on June 15, 2020, in accordance with the provisions of the

Article 28.2 of Regulation (EU) 2016/679, of April 27, 2016 -which

had the purpose of contracting the services of "Design, development, pi-

lotto and evaluation of a system that allows the traceability of contacts

in relation to the pandemic caused by Covid-19-.

The previous information and documentation provided for in section 1, is required

re in relation to the pilot test, from the beginning of the relative actions

to it, including the phase prior to its implementation and subsequent development.

later, until its completion.

2. Regarding the Radar COVID APPLICATION launched in the different

autonomous communities and cities after accession through the opportunities

bilateral agreements signed between the Ministry of Health and the Conse-

corresponding jeries:

b)

c)

a) Personal data required by the Radar COVID application to function

operate correctly and fulfill its purposes.

Information on the processing of such personal data, understood

as the set of operations performed on that data.

Information on the following question: What has the material-

Mind that data processing?

Specifically, the life cycle of the data processed, the process of these

from its collection to its deletion or blocking.

d) Documentation accrediting whether the protection delegate has been requested

tion of data from the Ministry of Health advice on the nature

legal validity of the data processed and the response, which, where appropriate,

have formulated.

e) Documentation accrediting the documented instructions directed

SEDIA or SGAD, in accordance with the provisions of article 28.3.a) of the

Regulation (EU) 2016/679, of April 27, 2016.

f) Copy of the record of personal data processing activities

made in the Radar COVID application. Said register, to which

re Article 30 of Regulation (EU) 2016/679, of April 27, 2016,

must be provided in its initial version, together with any additions, modifications,

cation or exclusion in the content of this.

g) Impact assessment(s) relating to data protection

regarding the Radar COVID application.

The information and documentation provided for in section 2 is required in relation to

tion with the commissioning of the Radar COVID application from the 10th of

October 2020, after the publication in the BOE of the Resolution of October 13

2020, of the Undersecretariat, by which the Agreement between the Mi-

Ministry of Economic Affairs and Digital Transformation and the Ministry of

Health, about the "Radar COVID" application.

On October 4, 2021, the notification was considered rejected after

ten calendar days from the availability of this without accessing its

contents.

After this unsuccessful notification attempt, the agreement was notified in

dated October 25, 2021, through the Correos postal service, according to evidence

of delivery that appears in the file.

FIFTEENTH: The DGSP in response to the notified evidence requirement,

He provided the following documents to the proceedings:

1. Operational aspects for the implementation of RADAR COVID in the Autonomous Communities, with

date of August 17, 2020.

2. List of integration of the RADAR COVID app in the Autonomous Communities, updated to date

of September 2, 2020.

3. Questions and answers about the contact tracing app Radar CO-

VID19, dated September 15, 2020.

4. Implementation procedure of the Radar COVID App as a complement to the

manual contact identification systems, version of August 15, 2020.

5. Implementation procedure of the Radar COVID App as a complement to the

manual contact identification systems, version of September 15,

2020.

6. Description and epidemiological value of the RADAR COVID solution, dated July

of 2020.

7. RADAR COVID app key generation service, dated August

2020.

8. Copy of COVID RADAR deployment indicators in the Autonomous Communities, updated to 22

September 2020.

9. RADAR COVID Data Protection Impact Assessment Report

prepared by INDRA, dated September 2020.

10. Ppt presentation SEDIA follow-up of the RADAR COVID pilot, dated 24

July 2020.

11. Presentation ppt follow-up of the SEDIA project, dated July 31,

2020.

12. Minutes of the meeting held on July 27, 2020 on Design, development, piloting

evaluation of a system that allows the traceability of contacts in relation to the

pandemic caused by Covid-19.

13. Minutes of the pilot closing meeting of the RADAR COVID app in La Gomera and upcoming

sos held on July 31, 2020

14. Summary of results of the pilot of the Radar COVID infection alert app,

prepared by SEDIA.

15. Minutes of the meeting on functionalities of RADAR COVID, of July 17,

2020.

16. Minutes of the meeting on functionalities of RADAR COVID, of July 14,

2020.

17. Minutes of the follow-up meeting on APP RADAR-Application to detect

covid-19 contacts, July 13, 2020.

18. Minutes of the presentation meeting of the COVID Radar Pilot – Pilot on the island of

La Gomera, dated July 10, 2020.

SIXTEENTH: The SGSDII in response to the notified evidence requirement,

He provided the following documents to the proceedings:

Report prepared by the SGSDII dated November 5, 2021

- Referral letter from the Chief of Staff of the SGSDII

-

- Document 1

- Document 2

- Document 3

- Document 4

- Document 5

- Document 6

- Document 7

- Document 8

- Appendix 2

- Annex 3

SEVENTEENTH: On January 25, 2022, the instructor of the procedure

formulates a resolution proposal, in which it proposes that, by the director of the AEPD,

sanctioned with a WARNING to the GENERAL DIRECTORATE OF PUBLIC HEALTH

BLICA for violation of the following articles:

- Articles 5.1.a) and 5.2 of the RGPD, typified in article 83.5.a) of the RGPD and in

article 72.1. a) of the LOPDGDD, for the sole purpose of determining the

prescription bolts.

- Articles 12 and 13 of the RGPD, typified in article 83.5.b) of the RGPD and in the

Article 72.1.h) of the LOPDGDD, for the sole purpose of determining the deadlines

of prescription.

- Article 25 of the RGPD, typified in article 83.4.a) of the RGPD and in the

Article 73 of the LOPDGDD in section d), for the sole purpose of determining

prescription periods.

- Articles 28.1 and 28.3 of the RGPD, typified in article 83.4.a) of the RGPD and in

Article 73 of the LOPDGDD in sections: k) and p), for the sole purpose of

determine the statute of limitations.

- Article 35 of the RGPD, typified in article 83.4.a) of the RGPD and in the

article 73 of the LOPDGDD in section t), for the sole purpose of determining

prescription periods.

On January 26, 2022, through the Electronic Notification Service and

Electronic Address Enabled, the resolution proposal is notified.

EIGHTEENTH: After the period granted for the formulation of allegations

to the proposed resolution of the procedure, it is found that no allegations have been received

tion by the DGSP.

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited

PROVEN FACTS

FIRST: Royal Decree 454/2020, of March 10, which develops the es-

basic organic structure of the Ministry of Health, and the Royal Decree is modified

139/2020, of January 28, which establishes the basic organic structure of the

ministerial departments was published in the BOE of March 12, 2020. Entered

in force on the same day of its publication in the BOE until August 6, 2020, the date

in which Royal Decree 735/2020 of August 4 came into force.

Article 3 provides:

1. The General Directorate of Public Health, Quality and Innovation is the body

that assumes the functions related to foreign health; the promotion of

health and the prevention of illness and injury; the coordination of the

public health surveillance; environmental health and occupational health; the development

of criteria, standards or requirements for authorization and quality of the centers and

health care services; interventions on equity and quality in the

health care system, through specific tools such as

be the coordination and development of the health strategies of the National System

end of Health; or transversal, such as the incorporation of projects of

equity in access to health technology or equipment, without prejudice to

those that they could hold in relation to them, other organizations, institutions,

tions or ministerial departments.

2. It is responsible for the development of information systems, the management of

information and identification of the protected population and access to information

clinical and therapeutic training, the promotion of health plans and training programs

ity in the National Health System, including the National Plan on AIDS,

as well as the analysis and evaluation of the functioning of the health system

storeroom and its comparison with other health systems. (…)".

SECOND: Royal Decree 463/2020, of March 14, declaring the state of

alarm system for managing the health crisis situation caused by CO-

VID-19, in article 4.2.d) designates the Minister of Health as the competent authority.

delegated to you in your area of responsibility.

THIRD: On March 28, 2020, the Order SND/

297/2020, of March 27, by which the Secretary of State for Di-

digitization and Artificial Intelligence, of the Ministry of Economic Affairs and Transformation.

Digital information, the development of various actions for the management of the health crisis

ria caused by COVID-19.

The first solver says:

First. Development of technological solutions and mobile applications for

collection of data in order to improve the operational efficiency of services

health services, as well as the best care and accessibility by citizens.

give us

1. Entrust the Secretary of State for Digitization and Artificial Intelligence

of the Ministry of Economic Affairs and Digital Transformation, the development

urgent development and operation of a computer application to support the

management of the health crisis caused by COVID-19. This application

will at least allow the user to carry out a self-assessment based on the symptoms

doctors you communicate, about the probability that you are infected by the

COVID-19, offer information to the user about COVID-19 and provide the

user practical advice and recommendations of actions to follow according to the

evaluation.

The application will allow the geolocation of the user for the sole purpose of ve-

Verify that you are in the autonomous community in which you declare to be. The

application can include within its content links to portals managed

ned by third parties in order to facilitate access to information and services

available through the Internet.

The application will not constitute, in any case, a medical diagnosis service,

emergency care or prescription of pharmacological treatments. The

The use of the application will not replace in any case the consultation with a pro-

suitably qualified medical professional.

The person responsible for the treatment will be the Ministry of Health and the person in charge of

treatment and owner of the application will be the General Secretariat of Administration

Digital tion. The Ministry of Health, as the controller, authorizes

encourages the General Secretariat of Digital Administration to resort to other

two in the execution of the provisions of this section.

2. Entrust the Secretary of State for Digitization and Artificial Intelligence

official, from the Ministry of Economic Affairs and Digital Transformation, the development

development of a conversational assistant/chatbot to be used via whatsapp and

other instant messaging applications. Will provide official information

to questions from citizens. The design will be based on information

official from the Ministry of Health.

The person responsible for the treatment will be the Ministry of Health and the person in charge of

treatment and owner of the chatbot will be the Secretary of State for Digitization and

Artificial Intelligence through the General Subdirectorate of Artificial Intelligence

Social and Digital Enabling Technologies.

3. Entrust the Secretary of State for Digitization and Artificial Intelligence

official, from the Ministry of Economic Affairs and Digital Transformation, the development

Development of an informative website with the technological resources available.

It is verified that the Radar COVID application is not included within the solutions

technology and mobile applications for data collection in order to improve

the operational efficiency of health services given their purpose, which is different: the

contact traceability.

Its purpose is extracted, among others, from:

-The "General Information" provided by the Government of Spain when it indicates: What is

COVID Radar?:

https://radarcovid.gob.es/faq-informacion-general

Radar COVID is a mobile application developed to help control the

spread of COVID-19 through the identification of possible con-

close touches of confirmed cases via Bluetooth technology.

From the Seventh “EXPOSE” of the Resolution of October 13, 2020, of the Undersecretary

which publishes the Agreement between the Ministry of Economic Affairs and

Digital Transformation and the Ministry of Health, about the application "Radar CO-

VID, which says:

Seventh.

That «Radar COVID» is an application for mobile devices that promotes

monitors public health through a COVID-19 infection alert system

19. The application, through the use of ephemeral random identifiers

that are unrelated to the identity of the mobile phone used or the

user, detects the strength of Bluetooth signals exchanged between devices.

devices that have this application downloaded and active, The device of each

user periodically downloads the Bluetooth keys of all users of

the application that they have informed through the same that they have been diagnosed-

ticated COVID-19 (prior accreditation of the competent health authorities)

tes), proceeding to determine if the user has established risk contact

with any of them, verified by the Bluetooth signals exchanged. Yes it is

case, the application notifies you of this fact, so that you can take me-

didas, and thus help prevent the virus from spreading.

FOURTH: In the month of April 2021, a meeting is held with the purpose of

address the "Design, development, pilot and evaluation of a system that allows the trace-

bility of contacts in relation to the pandemic caused by Covid-19".

The following people are involved:

Person

Dª C.C.C.

Ms D.D.D.

D.E.E.E.

D.F.F.F.

Ms. G.G.G.

Ms. H.H.H.

D.I.I.I.

D.J.J.J.

Ms. K.K.K.

D.L.L.L.

Mrs M.M.M.

C/ Jorge Juan, 6

28001 – Madrid

SEDIA / CCAA / Ministry of Health / Minsait

SEDIA

SEDIA

SEDIA

SEDIA

Ministry of Health

Ministry of Health

SEDIA

Canary Islands Government

Minsait

Minsait

Minsait

www.aepd.es

sedeagpd.gob.es

69/168

Person

Ms. N.N.N.

D. Ñ.Ñ.Ñ.

D.O.O.O.

The issues discussed are:

SEDIA / CCAA / Ministry of Health / Minsait

Minsait

Minsait

Minsait

The attached document 20200721_Seguimiento SEDIA v5 is presented, where

includes the executive summary of the conclusions of the analysis of the results of the

pilot.

The agreement adopted is:

It is agreed to have ready for next Tuesday 07/28/2020 the list of

actions to be carried out on the app in order to put it into production

imminent, either in a CCAA, city or at the national level. remember too

prepare a descriptive document with a summary of the operation of the

app so that the different Autonomous Communities can analyze its operation.

FIFTH: On May 6, 2020, the METD publishes the following press release:

“Spain works at a national and European level for the interoperability of applications

infection prevention measures against COVID-19.

The Third Vice President of the Government and Minister of Economic Affairs and

Digital Transformation, P.P.P., together with the Secretaries of State for Digitization

and Artificial Intelligence, C.C.C., and Telecommunications and Digital Infrastructures.

them, Q.Q.Q., participated in this meeting to seek a co-European position

that allows taking advantage of the possibilities offered by technology to con-

contribute to the management of the pandemic and the subsequent recovery at European level.

Among these digital solutions, the focus was placed on prevention applications

infection rate. In this sense, Spain highlighted the importance of finding a

coordinated approach at European level for these applications that guarantees the integration

operability and allow for a joint exit from the health emergency.

In addition, the need to take advantage of the potential offered by the economy was pointed out.

digital mine to contribute to the management of the pandemic, being necessary to find

a balance between the benefits derived from these innovations and privacy,

safety and ethical issues.”

SIXTH: On June 9, 2020, the General Director of Public Health, Quality

and Innovation of the MSND sent a letter to the Secretary General of Digital Administration

(SGAD) with the following tenor:

“In relation to the pilot test of the mobile application for the traceability of con-

COVID-19 tacts that are planned to be carried out in the Autonomous Community

Canary Islands, I inform you of the approval of this Ministry for its development.

To carry it out, in our opinion, it should be sent to the Agency

Spanish Data Protection all the information that corresponds to ga-

guarantee compliance with current regulations on this matter.

On the other hand, we understand that the person responsible for processing the data of

This pilot will be the health authority of the community in which it will be carried out.

cape.

Appreciating the work being carried out by the Secretary of State for Digitization

tion and Artificial Intelligence in the response to COVID-19, receive a cordial

greeting."

SEVENTH: On June 11, 2020, the already repealed Royal Decree entered into force.

to-law 21/2020, of June 9, on urgent prevention, containment and coordination measures

nation to deal with the health crisis caused by COVID-19.

Articles 5, 26 and 27, provided:

Article 5. Action plans and strategies to deal with health emergencies.

In accordance with the provisions of article 65 of Law 16/2003, of May 28, of

cohesion and quality of the National Health System, the adoption of

action plans and strategies to deal with health emergencies, through

coordinated actions in public health, attending to the different levels of

risk of exposure and community transmission of COVID-19 disease

for the development of the different activities contemplated in this royal decree-

law.

Article 26. Provision of essential information for the traceability of contacts.

The establishments, means of transport or any other place, center or entity
public or private entity in which the health authorities identify the need
ability to carry out traceability of contacts, they will have the obligation to provide the
health authorities the information they have or that is requested
regarding the identification and contact details of persons potentially
affected.

Article 27. Protection of personal data.

"1. The treatment of personal information that is carried out as con-
sequence of the development and application of this royal decree-law will be
in accordance with the provisions of Regulation (EU) 2016/679 of the European Parliament
and of the Council, of April 27, 2016, regarding the protection of natural persons.
cas with regard to the processing of personal data and the free movement
of these data and by which Directive 95/46/CE is repealed, in the Organic Law
3/2018, of December 5, on the Protection of Personal Data and guarantee of the
digital rights, and in what is established in articles eight.1 and twenty-three of the Law
14/1986, of April 25, General Health. In particular, the obligations of
training to the interested parties regarding the data obtained by the subjects included
within the scope of application of this royal decree-law shall comply with the provisions
placed in article 14 of Regulation (EU) 2016/679 of the European Parliament and
of the Council, of April 27, 2016, taking into account the exceptions and obligations
tions provided for in section 5.

2. The purpose of the treatment will be the monitoring and epidemiological surveillance of the
COVID-19 to prevent and avoid exceptional situations of special gravity,

attending to reasons of essential public interest in the specific field of

public health, and for the protection of vital interests of those affected and of other

natural persons under the provisions of Regulation (EU) 2016/679 of the

European Parliament and of the Council, of April 27, 2016. The data collected

will be used exclusively for this purpose.

3. Those responsible for the treatment will be the autonomous communities, the cities

from Ceuta and Melilla and the Ministry of Health, within the scope of their respective

competencies, which will guarantee the application of the security measures

that result from the corresponding risk analysis, taking into account

that the processing affects special categories of data and that such processing

These procedures will be carried out by public administrations obliged to comply

of the National Security Scheme.

4. The exchange of data with other countries will be governed by Regulation (EU)

2016/679 of the European Parliament and of the Council, of April 27, 2016, having

taking into account Decision No. 1082/2013/EU of the European Parliament and of the Council,

of October 22, 2013, on serious cross-border threats to the

health and the revised International Health Regulations (2005), adopted by the

58th World Health Assembly held in Geneva on May 23, 2005."

It is verified that this royal decree law does not enable the development of the Radar application

COVID.

EIGHTH: The "Condition specifications for the design, development, pilot and evaluation of

a system that allows contact tracing in relation to the pandemic caused

by Covid-19”, dated June 10 and 12, 2020, provides the following:

In section 1 under the heading "Background" it says:

Order SND/297/2020, of March 27, of the Minister of Health commissioned the

Secretary of State for Digitization and Artificial Intelligence (SEDIA), of the Ministry

Ministry of Economic Affairs and Digital Transformation, the development of di-

various actions for the management of the health crisis caused by CO-

VID-19. In particular, said Order establishes in its first resolution, the De-

development of technological solutions and mobile applications for the collection

of data in order to improve the operational efficiency of health services,

as well as the best care and accessibility by citizens.

Additionally, the General Directorate of Public Health, Quality and Innovation,

of the General Secretariat of Health (Ministry of Health) has given the Approval

OK to a pilot test of contact tracing in relation to COVID-19,

commissioning SEDIA to develop a mobile application for this purpose.

In section 2 under the heading "Object of the contract" it says:

 Pre-pilot phase:

o Technical analysis of the Contact Tracing System.

o Development of a first viable product.

or testing of it.

o Security audit.

o Optimization of adoption by the pilot group.

 Pilot phase:

o Usage tracking.

o Functional evolution of the App.

or Learning.

 Post-pilot phase:

o Functional evolution of the App with the learning obtained in the

previous.

 Cloud infrastructure:

o Platform of services required to host the Backend of the Application.

cation, in self-management mode.

NINTH: On June 15, 2020, the SGAD signs an emergency contract

cia with INDRA SOLUCIONES TECNOLOGÍAS DE INFORMACIÓN, S.L.U, which has

Its purpose is the contracting of services for the development of an application for

traceability of contacts in relation to the pandemic caused by COVID-19,

for an amount of 330,537.52 euros (VAT included).

TENTH: It is recorded, dated June 23, 2020 in the Reference of the Council of Mi-

Ministers, the following Agreement:

“AGREEMENT by which reason is taken of the declaration of emergency for the

contracting of the services of design, development, pilot and evaluation of a system

that allows contact tracing in relation to the pandemic caused by

COVID-19, with a duration of 5 months, for an amount of 330,537.52 euros,

VAT included."

“APPROVED THE DEVELOPMENT OF THE PILOT FOR A MOBILE APPLICATION

NOTIFICATION OF RISK CONTACTS FOR COVID-19.

The Council of Ministers has given the green light to the contract to design, develop and

evaluate a pilot test for a mobile application that allows notifying users

contacts of a user the possible risk of contagion by COVID-19. The objective

is that the Ministry of Economic Affairs and Digital Transformation, through

the Secretary of State for Digitization and Artificial Intelligence, and in coordination

with the Canary Islands Health Service, launch next week a

pilot test of this technological tool on the Canary Island of La Gomera. The

The objective of the pilot project is to evaluate technical and user experience aspects of the

citizen, in order to optimize the design of the application and its degree of trust.

whoa It will also serve to calibrate the app's algorithm in order to guarantee the

accuracy of notifications. Once the pilot test has been completed and evaluated in

a real scenario, the appropriate decisions can be made for the connection with

the health system of the different autonomous communities. this tool

technology adds to the measures already put in place by the authorities

to follow the contacts of COVID-19 infections and that, together with

the preventive measures adopted, are contributing to the control of the pande-

mine. The contract approved by the Council of Ministers through the emergency procedure

cia has subscribed with the company Indra Soluciones Tecnológicas de la Informa-

tion S.L.U. for an amount of 330,537.52 euros, VAT included."

ELEVEN: There is, dated June 23, 2020, a press release published by

the METD, with the following tenor:

"The Government approves the development of the pilot for a mobile notification application

tion of risk contacts by COVID-19. (…)

The objective is that the Ministry of Economic Affairs and Digital Transformation,

through the Secretary of State for Digitization and Artificial Intelligence, and in

coordination with the Canary Islands Health Service, launch the next series

A pilot test of this technological tool is emerging on the Canary Island of La

Slingshot. (…)

The Spanish Agency for Data Protection has participated in the preliminary process

to the start-up of this pilot and will also participate in the evaluation of the

results to be able to propose improvements that guarantee at all times the first

emptiness to users."

TWELFTH: On June 29, 2020, the Government of Spain launched the

pilot project that runs until July 31, 2020 on the island of La Gomera.

In the follow-up document dated 07.24.2020, the following phases and

COVID Radar pilot planning dates:

A report of conclusions has been published (***URL.6) prepared by SEDIA, fe-

dated January 28, 2021, indicating:

The app allows

• Verify the authorization code by the health authority before possible

positive for COVID-19

• Allows the user to transmit and receive random identifiers to

via bluetooth

• Sends its ephemeral key generating beacon to the server in case of positive

• Ask the server for the anonymous passwords of infected users in a temporary way.

rhodic

• Show notifications to the user with instructions on what to do in case of

who has been in contact with another COVID-19 positive user

Its development is supported by the Google & Apple alliance for the implementa-

mentation of a common API in charge of managing and providing the dis-

positive anonymous random keys and their exchange via bluetooth through

the following functions:

Manage daily random keys

• Generate daily temporary exposure keys and rotate the

ephemeral ids based on them

• Provides the keys to the application for diagnosed users, including

going temporary values

• Accepts app keys for exposure detection, including-

do the dates and levels of risk of transmission

• Store keys on the device

Manage Bluetooth sending and scanning

• Management of sending keys

• Scan keys issued by other devices

• Stores the observed keys in storage on the device.

tive

• Identifies when another user in contact has been a confirmed case

• Calculation and provides the risk of exposure to the application

• Presents the following permission requests to the user:

• Before you start scanning and sending the keys

• Before providing the server with the keys to the central server after

having been infected G

Objectives and methodology of the pilot

Duration:

• 15 days of active APP (monitoring phases and expansion of monitoring).

torization)

• Start date: Week of June 29 (communication and dissemination phase).

vulgation)

• End date: week of July 20 (conclusions analysis phase)

Location:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

San Sebastián de La Gomera (approximately 10,000 inhabitants including

residents, tourists and people who commute daily for reasons of

work), a municipality located on the Island of La Gomera.

Participants

• Residents in the municipality captured by different access channels

to the pilot.

• Visitors residing in Tenerife who traveled to the municipality during

before the pilot, captured by different access channels to the pilot.

Pilot Reach: Volume of participants

• The greatest possible participation will be promoted by combining different

access to it, estimating a volume between 2,000 and

3,000 APP users

• Approximately 10% of cases will be established with Positive in

Simulated COVID, to favor the detection of cases of risk and thus

check APP operation

Assessment of compliance with objectives

• Quantitative data analysis

• Qualitative analysis: anonymous surveys and remote user tests

(15 users)

Pilot Objective

(...) Thus, the objective of the pilot was to monitor the operation of the APP of

controlled way to:

1. Optimize the APP design (...)

2. Behaviors and preferences regarding prevention of citizens

we (...)

3. Contrast initial hypotheses (...)

4. Obtain insights for the deployment (...)

Scope

As mentioned above, the pilot has been planned from a

simulated and controlled perspective, so that conclusions can be drawn

of value with respect to its operation, use and behavior by the

citizenship, but limits the collection of data in relation to some aspects:

Open discharge vs controlled discharge

Although at first the possibility of controlling access to

the download of the application exclusively to the target audience of the pilot, resi-

residents, workers or visitors to San Sebastián de la Gomera, it was decided to fi-

leave it open

due to 3 key factors

finally

:

• Complexity of implementation.

• Negative impact on usability by citizens by having to in-

Enter access codes for the download.

• Incorporate a factor unrelated to the application's own operation in the sub-

post national deployment.

Privacy vs qualified information.

The pilot has followed the same premise that governs the application itself, the

guarantee of protection of personal data and anonymity in the use of Radar

COVID. Along these lines, aggregate information has been collected from users

of the application, both of the people who downloaded it, and of the

people who assumed the role of Positive Cases or received notifications of

contagion risk alert. This aggregate information prevents obtaining information

behavioral training or by more qualified profiles of citizens, as well

as a sociological analysis of virus spread.

Simulation vs Reality

The pilot strategy was based on a simulation of positive cases by

of volunteers who entered the code assigned to them, creating by

both a fictitious and forced propagation outbreak that does not allow pro-

actual payment of the disease that would be monitored by the application.

Methodology.

Pilot approach.

• Get the largest number of users possible, enabling different channels

of access to participation by the target citizens of the pilot.

• Incorporate participants from different population profiles to detect facilita-

different drivers and barriers to use.

• Prioritize checking the functionality and user experience of the APP

simulating a high volume of positive cases (10% of the estimate of

user population of the APP during the pilot) that would favor the generation of

pilot evaluation key KPIs, but maintaining an incident rate

epidemiologically reasonable predicted cumulative incidence

(2.2%).

• Maintain control of positive cases and introduction of codes in the

APP, limiting access only to controlled samples.

• Obtain direct feedback from pilot users to optimize the design.

No.

Monitoring and agility in decision making

In order to have continuous information on the evolution of the dis-

pilot indicators of success and redirect its focus if necessary

To achieve the final objective, different reporting tools were created and

control, which would make it possible to incorporate the data collected anonymously and

luntaria:

• Daily registration template for participants recruited by promoters,

collecting aggregated information on sex and age from the group of

sonas captured in each day of promotion.

• Daily template for the delivery of positive codes by promoters,

also providing aggregated information on the sex and age of the persons

which was assigned the role of positive volunteer.

• Daily call log template in CAU, according to the reason for the call.

madam

• Daily call content record template due to risk of aller-

ta, for which a call script was created.

• Global dashboard of key indicators of participants, codes

payments, notifications and other information specified in the paragraphs

do of conclusions.

The continuous monitoring of the information allowed to make agile decisions

such as the displacement of promoters to new areas in the face of possible saturation

ration of the initial areas or the incorporation of a new wave of infections

in shipping company

Results of the pilot Methodology for evaluating the effectiveness of Radar CO-

VINE

The relevant questions to evaluate the effectiveness of Radar COVID are:

User behavior and attitude towards the application, evaluating whether it has

served the purpose of Radar COVID based on:

Adoption Is Radar COVID achieving enough critical mass to be effective?

Are new versions of the app adopted?

Commitment and participation Is the user motivated and complies with the instructions?

n that facilitate the containment of the pandemic? Are you fast on the fulfillment

of the instructions? How positive is the photo when contrasted with initiatives?

Are you comparable in Europe?

Retention

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

78/168

Once installed, does the user continue with the application active and in use or, for

On the contrary, you lose interest and turn it off? Application performance in the

detection of the risk of contagion among citizens:

Outbreak Simulation How many close contacts can Ra-

give COVID for each positive case confirmed through the app?

Results that allow evaluating the effectiveness of Radar COVID

Adoption

Has a level of adoption been reached that allows conclusions to be drawn?

operation and effectiveness of Radar COVID?

The level of adoption achieved during the pilot has made it possible to verify the

operation of the application and test its effectiveness in positive cases of CO-

VID-19, although its result cannot be extrapolated to the national deployment, having

had a very high and targeted promotion level in the municipality.

At the end of the pilot, more than 58,000 downloads had been achieved.

such, 90% on Android, and only in the period of direct activation in San Se-

Bastián de la Gomera, between July 6 and 20, the figure is around 11,000

downloads.

Due to the limitations indicated in the previous section, it is not feasible to differentiate how many of these downloads belong to SS de La Gomera to confirm the target forecast of approximately 3,500 downloads in the municipality which would represent 35% adoption, although some estimates can be made information that would confirm having reached the desired threshold, being conservants in the forecast:

• “Assisted” downloads: 924. Downloads that have been carried out successfully. made by the promoting agents located both in the municipality of SS de La Gomera as in the collaborating boats in the pilot.

• Public employees: The participation of 758 public employees was encouraged of the 3 institutional spheres (La Gomera SS City Council, Cabildo of La Gomera and Health Services) and they were invited to also promote download it in your closest environment.

• If we assume that the participation rate is similar to the rate obtained from introduction of positive codes (61%) and that each public employee shares it met with an average of 3 people from his closest environment, we obtain a participation promoted by this group of some 1,850 users of the application tion.

• Spontaneous participation: If we consider that dissemination campaigns and promotion of the initiative carried out through press conferences, informative notes, activities, activity in social networks and information available in the planes of the BINTER company, will arouse the interest of the population of the municipality and agreed on a voluntary discharge of at least 2% of the population, it was

they would have gotten an additional 200 downloads.

• Web downloads of the Government of the Canary Islands: 241 clicks have been recorded on the link direct download ce on the web; we estimate that all clicks have materialized discharge 66 With these estimates, it can be concluded that the al- discharge rate stands at 3,215 and therefore has made it possible to evaluate the cacia and operation of Radar COVID, since the real final figure we estimate that can be between this minimum threshold of 3,215 and 11,675 downloads that have occurred during the duration of the pilot. It is worth noting that the rate of adoption is especially high, considering additionally that, of the 10,000 inhabitants of San Sebastián de La Gomera, approximately 10% of the population is under 10 years of age (lower age limit considered rada to have a smartphone and 11% are people over 75 years old where there could be a lower penetration rate of these devices, following the population distribution published by the INE corresponding to January 1, 2020 for the whole of the island of La Gomera. Extrapolating to the whole national population at the time of global deployment, it will be difficult to get this rate of adoption, although with a view to the pilot it has made it possible to carry out the analyzes necessary for the operation of the app.

THIRTEENTH: On July 10, 2020, a meeting called- "presentation of the COVID Radar Pilot - Pilot on the island of La Gomera Reu- Governance Committee follow-up meeting" to assess and discuss the state of situation of the COVID-19 Radar Pilot Project.

Members of various departments participate: the Secretary of State for Digitization and Artificial Intelligence, the Center for the Coordination of Health Alerts and Emergencies

tarias of the General Directorate of Public Health, Quality and Innovation (G.G.G. and R.-

R.R.), the General Directorate Modernization and Quality of Services, Canary Service

of Health, the Project Management, the Rovira i Virgili University and the Indra Team.

FOURTEENTH: On July 13, 2020, the follow-up meeting is held.

to about APP RADAR-Application to detect covid-19 contacts, with assistance

by the Ministry of Health: G.G.G., R.R.R. and S.S.S. July 2020; for another

side attendees: F.F.F., Deputy Director General for the Promotion of Digitization of the Administration

traction; TTT (sic), Cabinet of the Secretary of State for Digitization and Intelligence

Artificial Intelligence Representatives of the Indra project.

The minutes of the meeting state that:

"1. Background: the development of the RADAR App is put into context together with

with other initiatives of the Secretary of State such as the App “Assistance CO-

VID, Q&A Chat boot, informative portal covid19.gob.es or DataCovid (data

of telephony mobility and in collaboration with the INE).

(…)

4. Discussion. Discussion is generated around the following points: a) The idea

is that from the Ministry of Health we support the development of a single

app at a national level that can later have interoperability at a European level

since the authorization to access the API depends on the Ministry. There is

least 4 CCAA that have asked Apple and Google to develop their own tool

lies and there is a risk that this will happen if the national project does not happen in

time and manner"

FIFTEENTH: On July 14, 2020, a meeting is held regarding the

RADAR COVID functionalities, which includes the following: “Attendance: U.U.U.,

S.S.S. and G.G.G.: Coordination Center for Health Alerts and Emergencies. Direction

General Office of Public Health, Quality and Innovation R.R.R.: Support Unit. Direction

General Education of Public Health, Quality and Innovation. They participate in the meeting

members of the Secretary of State for Digitization, responsible for the pilot project in

Canary Islands and representatives in the CCAA of the interoperability group of the application

tion. Introduces the meeting F.F.F., Deputy Director General for the Promotion of Digitization

of the administration. Continua O.O.O., responsible for the project developed by IN-

DRA with a presentation of the pilot study that is being developed in the municipality

San Sebastián de La Gomera in the Canary Islands”.

According to the minutes of the aforementioned meeting, it is stated that:

“SEDIA clarifies that there is a mandate from the Ministry of Health and it is de-

It is desirable that the application be implemented at the same time throughout the national territory.

nal. This implementation is expected to be carried out in the months of September.

bre-october. Several Autonomous Communities ask about the possibility of carrying it out in waves.

given since there are some who would like to start the process in the month of

August. SEDIA comments that they have some pending audits and that in

As soon as they are closed, the application can be launched nationwide. They clarify that the

code emission model that is chosen will also condition the speed

with which the project can be launched at the national level.

(…)

Several autonomous communities (Catalonia and Aragon) ask about the analysis

of risks and evaluation of the impact, as well as the validation on the guarantee

application data protection. Are you wondering about the warranty issue?

of data protection and SEDIA clarifies that there is no data record

personal, they are pseudonymized data, no device is identified

no user and records are deleted after 14 days.

(…)

Murcia asks if there is a possibility of exploiting the information on movements and

geolocation or the origin of the cases to know if they are imported or not.

From SEDIA they clarify that it is an application that does not allow analysis

statistics, identification of cases or geolocation of devices, the information

The information collected by the application is anonymous, it does not recognize citizens or locations.

tions.”.

SIXTEENTH: On July 17, 2020, a meeting is held regarding the

functionalities RADAR COVID July 17, 2020, to which again participate:

“Attendance: U.U.U., S.S.S. and G.G.G.: Center for the Coordination of Alerts and Emergen-

Sanitary companies. General Directorate of Public Health, Quality and Innovation R.R.R.: Uni-

support. General Directorate of Public Health, Quality and Innovation. participate

at the meeting members of the Secretary of State for Digitization, responsible for

pilot project in the Canary Islands and those responsible for the project at INDRA”.

SEVENTEENTH: There is a document called “Radar COVID. Tracing:

07.24.2020” prepared by SEDIA together with the Canary Islands Health Service, the Government of

Canary Islands, the Government of the Cabildo de La Gomera and the City Council of San Sebastián

of La Gomera, where the following is reported:

Escalation and integration with Health Services

After reco***TOOL.1 proposals from the Autonomous Communities,

we opted for a centralized code generation scheme and managed

decentralized tion

Analysis of data.

The results of the pilot have been analyzed based on:

- Degree of adoption and retention

- Participation and simulation of waves

- Close contact detection

- User Feedback

What conclusions do we draw about the success of the pilot?

Users continue to use Radar COVID once installed, such as

shows the log of active apps: 12,700 active apps on average, with

a variation of +/-5% between its highs and lows (13,417 and 12,116)

Radar COVID cumulative downloads: 58,652

EIGHTEENTH: There is a "Summary of results of the alert app pilot

Radar COVID infections, prepared by SEDIA, dated 07/27/2020, where

They point out as main arguments:

The most notable ideas about the usefulness of the app:

• Radar COVID is a complement to manual tracing and to the measures and recommendations

health recommendations

• This app can help with the urgency of incorporating manual tracers.

them

• The app sees more than us (we would only remember known contacts).

cids, the app also the unknown ones)

• The app is faster than us (contacts are registered and

positive by proactively updating every day)

• The app has more memory than us (it registers any close contact).

cano, even those that can go unnoticed by us)

• The app is more anonymous and less intrusive (maximum privacy standards).

much less intrusive than getting a call from someone you

reconstruct what you have done in the last fifteen days)

NINETEENTH: On July 31, 2020, the meeting called

pilot closure of the RADAR COVID app in La Gomera and next steps with the participation of

“Assistance from the Ministry of Health: V.V.V., W.W.W.: Coordination Center for

Health Alerts and Emergencies. General Directorate of Public Health, Quality and Inno-

ration R.R.R.: Support Unit. General Directorate of Public Health, Quality and Inno-

vacation. Members of the Secretary of State for Digitization participate in the meeting

(including F.F.F., Deputy Director General for the Promotion of Digitization of the Administration-

tion), and responsible for the pilot project in the Canary Islands and the programming of the app

of the INDRA group.

The minutes of the meeting state that “the following responsibilities are assigned to the Mi-

Ministry of Health: Validation Analysis Report of Conclusions. (…) Group of

Work Ministry of Health + CCAA + SEDIA (procedures, code management,

action protocols,…”.

TWENTIETH: There is a document called “Radar COVID. Tracking pro-

project 07.31.2020”, where SEDIA defines the recommended launch activities

you give for the roll out:

TWENTY-FIRST: The document entitled "COVID Radar: Description and epi-

demiological of the solution" of July 2020, prepared by SEDIA.

Regarding security and privacy, it is stated that:

"It complies with the maximum security and privacy requirements, since when using

Bluetooth to search for other mobile phones that also have insta-

Open the application, it is not necessary to reveal the identity, the telephone or the mail

email of the user, or the location where the user is.

The app has a data management process with privacy by design.

year, ensuring at all times the anonymity of users, according to the norm

current regulations and European standards.

The privacy measures contemplated in the solution are the following:

• No login is required, nor is the user asked for any personal data to be identified.

captive or not

• The user can deactivate the app whenever he wants.

• In order to record the interactions between devices in an anonymized way,

generate changing random identifiers that preserve the identity of

the devices.

• Access to the data of said interactions is made only when

a new COVID-19 positive is diagnosed.

• The data is stored in a decentralized manner for a period of 14

days, after which they are deleted.

• Notifications to users exposed to Covid-19 are generated in the

app, without requiring to identify the user's device or phone number".

This document includes various questions and answers and, in relation to

personal data and privacy it is pointed out that,

"Here is a list of some of the measures with which Radar COVID

protect your data:

• The application does not collect any data that allows you to trace your identity. By

example, will not ask you and will not be able to know your name, surnames, address,

phone number or email address.

• The application does not collect any geolocation data, including that of the

GPS. In addition, it does not track your movements.

• The Bluetooth Low Energy code that is transmitted through the Bluetooth

The application is generated randomly and does not contain any informa-

tion on your smartphone or on you. Also, this code changes several times

every hour to further protect your privacy.

• The data stored on your mobile phone is encrypted.

• The connections between the application and the server are encrypted.

• All the data, both those that are saved in the device (codes exchanged

used with other mobile phones) are deleted after 14 days.

• Likewise, the data collected on the server, coming from the telephones

phones where a positive diagnosis for COVID-19 has been reported, are eliminated

mined after 14 days.

• No data stored on mobile phones or on the server allows the

identification neither of the mobile device itself nor of its user".

TWENTY-SECOND: On August 3, 2020, the METD publishes this note of

press:

"The Radar COVID contagion alert mobile application passes its testing phase.

bas fulfilling all the objectives set. (…)

This is what the Secretary of State for Digitization and Artificial Intelligence has explained.

officer, C.C.C., at a press conference in which he shared the results obtained

had during the pilot.

Together with her they have also intervened

***TOOL.1 Aparicio, general director of Public Health and Innovation of the

Ministry of Health, T.T.T. Hernández, General Director of Modernization and Ca-

ity of the Services of the Government of the Canary Islands, F.F.F., deputy director general of Im-

pulse of the Digitalization of the Administration, and E.E.E., technical advisor of the pro-

project."

Adoption, engagement, retention and performance success.

The test started on June 29 and has been developed until this past

July 31, time during which four waves of fictitious outbreaks have been simulated.

COVID-19 tices. During its development, and despite the fact that it only worked in the

island of La Gomera, more than 60,000 people downloaded the app throughout Spain.

The first objective of the pilot was to precisely evaluate the adoption of the

tool, that is, the number of people who would download it, and a target was set

goal of 3,000 participants for La Gomera, a goal that has been exceeded according to

the data obtained during the test.

A second objective was to measure retention, referring to the number of

users who kept the app active after downloading it. The re-

The results, also satisfactory, point to an average retention rate of 83%

zada.

In addition, the commitment of users in the communication of positions was analyzed.

fictitious assets, achieving 61% of active communications, of which 78%

occurred within 24 hours of receiving the contagion code if-

mulatto.

Another of the objectives outlined in the pilot was to measure the operation of the app

in contact tracing, achieving an average of 6.4 close contacts of

risk detected by confirmed simulated positive. That figure is almost double

current efficiency of manual tracers, which in the Canary Islands detect a

average of 3.5 contacts. (…)

TWENTY-THIRD: On August 5, 2020, it is published in the Official Gazette

of the State the Royal Decree 735/2020, of August 4, by which the es-

basic organic structure of the Ministry of Health, and the Royal Decree is modified

139/2020, of January 28, which establishes the basic organic structure of the

ministerial departments.

In the preamble of royal decree 735/2020, it is said:

“(…) In order to effectively undertake these new measures, as well as

in order to cope with the increased workload in the Ministry

of Health as a result of the pandemic caused by COVID-19, it is necessary to

It would be necessary to reinforce the structure of said Department. For this reason, through the Real

Decree 722/2020, of July 31, which modifies the Royal Decree

2/2020, of January 12, by which the ministerial departments are restructured

rials, the creation of a new Secretary of State for Health was established,

with the aim of strengthening the exercise of competences in matters of

constitutionally reserved to the General Administration of the State

do.

By means of this royal decree, the structure of the

Ministry of Health, contemplating the creation of the General Secretariat of

Digital Health, Information and Innovation of the National Health System, of the

which will depend on the General Directorate of Digital Health and Information Systems

tion for the National Health System, with the aim of addressing the projects

modernization, improvement and transformation of the National Health System,

in light of the new challenges arising from the pandemic caused by CO-

VID-19, and in particular those related to digital health, interoperability

and network services at a national, European and international level, as well as

health information systems, promoting the incorporation of

features of emerging next-generation technologies, such as

data analysis (“big data”), artificial intelligence or predictive analytics,

among others, in the field of health.”

Likewise, the first final provision of Royal Decree 735/2020 provides:

“Modification of Royal Decree 139/2020, of January 28, which establishes

establishes the basic organic structure of the ministerial departments.

Article 16 of Royal Decree 139/2020, of January 28, is modified by the

which establishes the basic organic structure of the ministerial departments

rials, which is worded as follows:

«Article 16. Ministry of Health.

1. The Ministry of Health is structured into the following superior bodies and

directors:

A) The Secretary of State for Health, on which the following bodies depend

managerial gains:

1. The General Directorate of Public Health.

2. The General Directorate of the Common Portfolio of Services of the National System

of Health and Pharmacy.

3rd The General Directorate of Professional Regulation.

4th The Government Delegation for the National Plan on Drugs, with rank

of General Management.

B) The General Secretariat of Digital Health, Information and Innovation of the System

National Health Department, with the rank of Undersecretary, on which the Di-

General Directorate of Digital Health and Information Systems for the

National Health.

C) The Undersecretariat for Health, to which the General Technical Secretariat depends.

nica.

2. The General Secretariat for Health and Consumer Affairs and the Secretariat

General Health Office, as well as the General Directorate of Public Health, Ca-

Quality and Innovation and the General Directorate of the Basic Portfolio of Services of the

National Health and Pharmacy System."

The functions of the DGSP are stated in article 3 of Royal Decree 735/2020, which states:

1. The General Directorate of Public Health is the body that assumes the func-

nes relating to foreign health; health promotion and prevention of

illnesses and injuries; coordination of public health surveillance;

(...).

It is verified that the provision contained in Royal Decree 454/2020, of 10

March, in article 3.2 regarding that "It is responsible for the development of

of information, the management of information and the identification of the protected population.

gives and access to clinical and therapeutic information", is now attributed to the SGSDII

in article 7.1 of royal decree 735/2020, which says:

Article 7. The General Secretariat of Digital Health, Information and Innovation of the

National system of health.

1. The General Secretariat of Digital Health, Information and Innovation of the System

The National Health Institute is the governing body of the Department responsible for

It is necessary to address projects of modernization, innovation, improvement and transformation

mation of the National Health System in light of the new challenges arising

of the COVID-19 pandemic, particularly those related to digital health

such and information systems. Also, it is up to you to carry out

activities aimed at transferring innovation and advances in research

tion to the National Health System, without prejudice to the powers conferred

given to the Ministry of Science and Innovation and to the autonomous communities. You

It also corresponds to the elaboration of information systems, the

information management and identification of the protected population and access

so to clinical and therapeutic information. It is also responsible for the control of the

health information, in the area of competence of the Department

.

The following competencies are verified in favor of the SGSDII attributed in the paragraphs

d) and j) of article 7.4 of Royal Decree 735/2020:

d) Carry out the necessary actions for the development and maintenance of the System.

topic of Health Information of the National Health System defined in the chapter

Title V of Law 16/2003, of May 28, on cohesion and quality of the National System

National Health Service, guaranteeing its standardization, comparability, transparency and

accessibility within the legal framework of personal data protection. (…)

j) Coordinate and supervise the data protection policy in compliance with the

regulations applicable to this matter within the scope of the powers of the Department

ment.

It is verified that the SGSDII does not intervene in the development of the pilot project since

It is created with Royal Decree 735/2020, of August 4.

TWENTY FOURTH: In the initial version of the "Privacy Policy of the Application

Radar COVID" published on August 7, 2020 together with version 1.0 of the app

Radar COVID (pilot version), contains the following information:

PRIVACY POLICY OF THE APP Radar COVID

Please read this privacy policy for users of the website carefully.

mobile application "Radar COVID" (or the "Application"), where you can find

all information about the data we use, how we use it and what it contains

troll you have on them.

IMPORTANT ANNOUNCEMENT:

The USER is warned that the use of the Application DOES NOT CONSTITUTE

YOU DO NOT UNDER ANY CIRCUMSTANCES A MEDICAL DIAGNOSIS SERVICE,

EMERGENCY CARE OR TREATMENT PRESCRIPTION

PHARMACOLOGICAL, since the use of the Application could not in any way

replace the personal face-to-face consultation with a medical professional

duly qualified.

1. What is COVID Radar?

Radar COVID is an application for mobile devices of alert of conta-

SARS-CoV-2 virus, whose HOLDER is the General Secretariat of Admi-

Digital Administration, dependent on the Secretary of State for Digitization and

Artificial Intelligence of the Ministry of Economic Affairs and Transformation

Digital.

Thanks to Radar COVID, those users who have downloaded the app-

tion and accept its use will receive a notification in the event that in the fourteen

days prior to that notification have been exposed to an epidemic contact

myological (less than two meters and more than 15 minutes) with another user (all

anonymous) who has declared in the application to have given a result

do positive in the COVID 19 test (prior accreditation of the authorities

sanitary). The application will inform you exclusively about the day (within

those previous fourteen) in which exposure to contact

but not about the identity of the user to whom it has been exposed (information

tion impossible as it is an application that does not request, use or store data from

personal character of the users) nor the identification of the device of this, nor

about the time or place where the exposure occurred.

Once a notification is received, the application will provide the exposed user with information

tion for the adoption of preventive and assistance measures, to contribute

thus to contain the spread of the virus.

The success of the application as a tool that contributes to the containment of

spread is directly linked to users being aware,

and act accordingly, that, despite communicating to the application

that a positive result has been obtained in the COVID 19 test (prior

accreditation of the health authorities) is voluntary, not communicating it and

being a mere receiver of information from third-party users makes the application

tion loses its preventive usefulness not only for other users but for the

rest of the general population. The completely anonymous character should

encourage, without a doubt, the exercise of this responsible action.

2. How does the app work?

Once you have downloaded the application, accept the conditions of

use and privacy policy and start using it, your mobile device generates

will generate each day a pseudo-random identifier called an "exposure key".

temporary" with a size of 16 characters (16 bytes or 128 bits) that will serve

to derive the "Bluetooth ephemeral identifiers" that are exchanged

with other nearby mobile phones that also have the app downloaded.

RadarCOVID cation.

"Bluetooth ephemeral identifiers" are pseudo-random codes with a

size of 16 characters (16 bytes, or 128 bits), which are generated by your phone

mobile every 10-20 minutes, based on the daily “temporary exposure code”.

These codes do not contain personal information that allows the user to be identified.

mobile phone or the user thereof. These “Bluetooth ephemeral identifiers”

are transmitted by your mobile phone several times per second to devices

nearby, accessible through Bluetooth Low Energy, producing an inter-

changing random codes between devices so they can be stored

ned by nearby phones that have downloaded the app. same

way, every five minutes, your mobile phone will listen to the effective identifiers

Bluetooth devices that are transmitted by other mobile phones that have

the application and will store them to calculate if you have been with another user con-

infected with COVID-19 in the last 14 days.

Your phone stores the temporary exposure keys that you have generated in

the last 14 days. Remember that these keys are randomly generated and not

They serve to identify your mobile phone or its USER.

If you have received a positive diagnosis for COVID-19, you can enter volunteers

maryly in the application the "single-use confirmation code" that you

will facilitate your Public Health Service and that will be validated on our server.

At that time, the application will ask for your consent to send to

our server the last 14 temporary exposure keys stored in

your phone, therefore, only if you lend it, these will be sent to the application server.

cation that, after verifying the accuracy of the code, will serve to compose

Have a daily list of keys for temporary exposure of infected people

by COVID-19 that are downloaded daily from the server by all

the Radar COVID applications that are in operation.

C/ Jorge Juan, 6

28001 – Madrid

The information in these listings is used so that on your own phone you can

check if you have had close contact (less than two meters and more than 15

minutes) with people who have reported a COVID-19 infection, without identity.

tify neither the person, nor the place of exposure, nor the mobile device, nor any-

any personal information about you or the other person. That is, the application downloads

voluntarily shared temporary exposure keys periodically

by users diagnosed by COVID-19 of the server, to compare them

with the random codes recorded in the previous days as a result of

contacts with other users. If a match is found, the application

runs an algorithm on the device that, based on the duration and distance

estimated contact, and according to the criteria established by the

health authorities, decides whether to display a notification on the device

of the user exposed to the risk of contagion, warning him of the contact, communication

giving him the date of the same and inviting him to self-isolate, and contact the

health authorities.

These keys sent to the server do not allow the direct identification of the

users and are necessary to guarantee the correct functioning of the system.

contagion alert ma

3. What data do we process about you?

The data handled by the application does not allow the direct identification of the

user or your device, and are only those necessary for the sole purpose of information

Mars that you have been exposed to a situation of risk of contagion by the

COVID-19, as well as to facilitate the possible adoption of preventive measures

and assistance.

In no case will the movements of USERS be tracked, excluding

thus any form of geolocation.

As part of the COVID-19 contagion alert system, data will be processed

the following data for users who have tested positive for COVID-19

for the purposes specified below:

The temporary exposure keys with which the user's device has generated

generated the random codes sent (Bluetooth ephemeral identifiers), to

devices with which the user has come into contact, up to a maximum

mo of the previous 14 days. These keys have nothing to do with the identity

entity of the USER, and are uploaded to the server so that they can be downloaded

by similar applications held by other users. With these keys,

through a processing that takes place in the mobile phone in a descending way.

processed, the USER can be warned about the risk of contagion for having

been in recent contact with a person who has been diagnosed with

COVID-19, without the application being able to derive your identity or the place where

contact took place.

A 12-digit one-time confirmation code provided by the authorities

health authorities in case of a positive test for COVID-19. This code must

be informed by the user to allow the voluntary loading of passwords

server exposure.

Voluntary questionnaire to collect information on the experience of

use of the application, understanding of it or perception of privacy

dad among others.

All information will be collected for strictly public interest purposes.

the field of public health, and in the event of a health emergency, decrees

tada, in order to protect and safeguard an interest essential to the lives of the

people, in the terms described in this privacy policy.

The applicable legislation is listed below:

Regulation (EU) 2016/679, of April 27, 2016, regarding the protection of

natural persons with regard to the processing of personal data and

the free movement of these data and repealing Directive 95/46/EC

(General Data Protection Regulation).

Organic Law 3/2018, of December 5, on the Protection of Personal Data and

guarantee of digital rights.

Law 14/1986, of April 25, General Health

Organic Law 3/1986, of April 14, on Special Measures in the Matter of

Public health.

Law 33/2011, of October 4, General Public Health.

Royal Decree 463/2020 of March 14, declaring the state of

alarm for the management of the health crisis situation caused by CO-

VID-19 that attributes to the Minister of Health the necessary competence in all

the national territory.

Ministerial Order SND/297/2020 of March 27, entrusting the

the Secretary of State for Digitization and Artificial Intelligence, of the Ministry

of Economic Affairs and Digital Transformation, the development of new ac-

tuations for managing the health crisis caused by COVID-19.

4. How do we obtain and where does your data come from?

The positive confirmation code for COVID-19 provided by the Service

Health Public. This will allow the upload to the server of the alert system of

contagions the temporary exposure keys with which the user's device

rio has generated the random codes sent (ephemeral identifiers Blue-

tooth), to the devices with which the user has come into contact, up to

a maximum of 14 previous days. These keys are only uploaded to the server

dor with the explicit and unequivocal consent of the USER, having entered

duced a positive confirmation code for COVID-19.

5. For what and why do we use your data?

The collection, storage, modification, structuring and, where appropriate, elimination

nation, of the data generated, will constitute treatment operations carried out

carried out by the Holder, in order to guarantee the correct functioning

use of the App, maintain the service provision relationship with the User.

rio, and for the management, administration, information, provision and improvement of the service

vice.

The information and data collected through the Application will be treated with

purposes strictly of public interest in the field of public health, given the

current health emergency situation as a result of the pandemic

of COVID-19 and the need for its control and spread, as well as to gain

guarantee your vital interests or those of third parties, in accordance with the regulations

current data protection.

For this purpose, we use your data to provide you with the "Radar COVID" service and

so that you can make use of its functionalities in accordance with its conditions.

tions of use. In accordance with the General Regulation for the Protection of

Data (RGPD) as well as any applicable national legislation, the

General Secretariat of Digital Administration will treat all the data generated

while using the App for the following purposes:

Offer you information on contacts considered to be at risk of exposure to

the COVID-19.

Provide you with practical advice and recommendations for actions to follow

According to situations of risk in the face of quarantine or self-quarantine,

I had

This treatment will be carried out through the alert functionality of

contagion that allows to identify situations of risk for having been in

close contact with users of the application who are

infected by COVID-19. In this way you will be informed of the measures

which should be adopted later.

6. How long do we keep your data?

Temporary Exposure Keys and Ephemeral Bluetooth Identifiers

are stored on the device for a period of 14 days, after the

which are eliminated.

Likewise, the temporary exhibition keys that have been communicated to the

server by USERS diagnosed as positive for COVID-19 also

They will also be removed from the server after 14 days.

In any case, neither the temporary exposure keys nor the ephemeral identifiers

Bluetooth ros contain personal data and do not allow identifier

users' mobile phones.

7. Who has access to your data?

Neither the “Radar COVID” application nor the contagion alert server store

personal data of any kind.

The data managed by the mobile application (daily exposure keys

temporary and ephemeral Bluetooth identifiers) are stored only in the

user's device for the purpose of being able to make calculations and derive reports

the USER about their risk of exposure to COVID-19.

Only in the case of reporting a positive diagnosis for COVID-19, the keys

of temporary exposure of the last 14 days generated on the device, and

under the explicit and unequivocal consent of the USER, are uploaded to the ser-

viewer for dissemination to all USERS of this system.

These keys have nothing to do with the identity of the devices

mobile phones or with personal data of the USERS of the Application.

8. What are your rights and how can you control your data?

Since the Radar COVID app does not store personal data, they are not

of application the rights of access, rectification, deletion, limitation, oppo-

position and portability, as well as not to be subject to decisions based solely on

mind in the automated processing of your data.

In any case, we are obliged to indicate that we assist you at all times.

the right to file a claim with the Spanish Protection Agency

Information Data (www.aepd.es).

9. How do we protect your data?

The Radar COVID system does not store personal data.

In any case, the security measures implemented correspond to the

provided for in Annex II (Security measures) of Royal Decree 3/2010, of 8

of January, which regulates the National Security Scheme in the field of

of the Electronic Administration.

Finally, we inform you that both the storage and the rest of the

Non-personal data processing activities used will always be

located within the European Union.

10. What is the legitimacy for the treatment of your data?

The generated data will be treated legitimately with the following legal bases-

them:

The free, specific, informed and unequivocal consent of the user of the

USER, making this privacy policy available to you, which

You must accept by marking the box provided for this purpose.

Reasons of public interest in the field of public health, such as the protection

against serious cross-border threats to health (article 9.2 i) of the

RGPD), for the treatment of health data (for example, the state of

an infected person or information about symptoms, etc.).

Fulfillment of a mission carried out in the public interest or in the exercise of

public powers conferred on the data controller (article 6.1 e)

GDPR).

Archive purposes of public interest, scientific or historical research purposes

or statistical purposes (article 9.2 j) RGPD).

The Owner of the Application may give access or transmit the data to third parties

service providers, with whom it has signed agreements to order

data processing, and that they only access said information to

provide a service in favor of and on behalf of the Controller.

11. What do you have to take into account especially when using "Radar COVID"?

You must take into account certain aspects related to the minimum age of

use of the Application, the quality of the data you provide us, as well

such as uninstalling the Application on your mobile device.

Minimum age of use: to be able to use "Radar COVID" you have to be

over 18 years of age or have the authorization of your parents and/or legal guardians.

them. Therefore, by registering in the Application, you guarantee the Owner that you are

older than that age or, otherwise, that you have the aforementioned autho-

torization

Quality of the data you provide us: the information you provide us in

the use of the Application services must always be real, truthful and es-

updated tar.

Uninstallation of the Application: in general, there can be two situations in

those that proceed to the technical deactivation of the Application on your device:

1) that you do it voluntarily, and 2) that the Holder proceeds to the

technical deactivation of the Application on your device (e.g. in cases where

that we detect that you have breached the conditions of use of the Application).

12. Cookie Policy

We only use technical cookies that allow the user to navigate and

the use of the different options or services offered in the Application

tion, such as accessing restricted access areas or using electronic elements.

safety measures during navigation.

I have read the document PRIVACY POLICY OF THE APPLICATION "Ra-

give COVID."

TWENTY FIFTH: In the initial version of the "Terms of Use of Radar

COVID" contains the following information:

Radar COVID TERMS OF USE

BY DOWNLOADING AND USING THE "Radar COVID" MOBILE APPLICATION MANI-

PARTIES THAT YOU HAVE READ AND ACCEPT THESE TERMS OF USE AND

THE PRIVACY POLICY. HERE IS ALL THE INFORMATION

REGARDING YOUR RIGHTS AND OBLIGATIONS AS A USER OF

THIS APPLICATION.

IMPORTANT ANNOUNCEMENT:

• The USER is warned that the use of the Application DOES NOT CONS-

IN NO CASE DOES IT CERTIFY A MEDICAL DIAGNOSIS SERVICE, OF

EMERGENCY CARE OR TREATMENT PRESCRIPTION

PHARMACOLOGICAL, since the use of the Application could not in any way

replace the personal face-to-face consultation with a medical professional

duly qualified.

1. What is COVID Radar

Radar COVID is an application that promotes public health through a

COVID-19 infection alert system, making available to

USERS (hereinafter, individually, the "USER", and jointly the

"USERS"), the possibility of browsing the Application, accessing the

contents and services of Radar COVID, in accordance with these CONDITIONS.

TIONS OF USE.

Radar COVID detects the strength of Bluetooth signals exchanged between

devices that have this active application, through the use of identifiers

ephemeral random factors, unrelated to the identity of the phone.

mobile phone employee or the USER. The device of each USER downloaded

Periodically generate the Bluetooth keys of all the USERS of the application.

tion that they have reported through the same that they have been diagnosed

COVID-19 (prior accreditation of the health authorities), proceeding to

determine if the USER has established risk contact with any of the

them, verified by the Bluetooth signals exchanged. If this is the case, the

cation notifies you of this fact, so that you can take action, and contribute

Build in this way to prevent the virus from spreading.

2. Use of COVID Radar

To use the Radar COVID services, it is a necessary requirement that

the USER authorizes the activation of the Bluetooth communications system of

low energy by the Application, after downloading it.

The USER accepts without reservation the content of these CONDITIONS

OF USE. Consequently, the USER must carefully read the same

more before accessing and using any Radar COVID service

under your entire responsibility.

IMPORTANT NOTICE: The use of the Application is free, free and voluntary.

would for all citizens. To use Radar COVID it is not necessary to be-

be registered, nor provide any personal, identifying or non-identifying data.

By activating the application, the USER accepts:

a) sending anonymously emitted Bluetooth signals by your device;

b) the reception and storage of Bluetooth signals from applications

compatible with Radar COVID, which are kept anonymous and decentralized

stored on USERS' devices for a period not exceeding 14

days;

and c) the information offered to the USER about the possible risk of contagion,

without personal data of any kind being referred to at any time.

The USER can voluntarily inform the application of a result

positive in your COVID-19 tests using the confirmation code of

a single use facilitated by the health authorities. The validity of this code

will be checked by the health authorities to ensure the correct functioning

Radar COVID lien. The USER will report the results of their tests.

bas and you will be asked for your express and unequivocal consent to share the

keys generated daily on your device, and corresponding to the last

We have 14 days. These keys are communicated to a server that will put them

provision of the Radar COVID suite of applications for download. The

communicated keys have no relation to the identification of the device.

site or the USER.

There will be no discrimination against potential patients who require

ran health services and have not used the application.

3. Security and privacy

The security measures implemented correspond to those provided for in the

Annex II (Security measures) of Royal Decree 3/2010, of January 8, by the

which regulates the National Security Scheme in the field of the Administration

Electronic tration.

We inform you that your data will be treated in accordance with the provisions of the

Privacy Policy of the Application, the full content of which can be found

See the following link: Privacy Policy.

All information will be treated strictly for purposes of public interest in the

field of public health, and in view of the health emergency situation decreed

in order to protect and safeguard an interest essential to the lives of persons

sonas, in the terms described in the privacy policy.

The information on the activity of the USERS is anonymous and in no way

At this time, USERS will not be required to provide any personal data. At all times, the

USER can disable the Bluetooth contact tracing system in the

application, as well as uninstall the same.

4. Change of service and termination

Radar COVID is always trying to improve the service and seeks to offer func-

useful additional features for the USER, always bearing in mind the

preservation of public health. This means that we can add new

functions or improvements that in no case will imply the processing of personal data.

as well as remove some of the features. If these actions affect

materially to the rights and obligations of the USER, will be informed to

through the Application.

The USER can stop using the application at any time and for

any reason, by uninstalling it from your device.

5. App Holder

The General Secretariat of Digital Administration (SGAD), dependent on the Sec-

Secretary of State for Digitization and Artificial Intelligence of the Ministry of

Economic Affairs and Digital Transformation, is the HOLDER of the application

COVIDRadar.

Radar COVID in its architecture uses the new framework provided by

Apple and Google developed from the DP-3T Protocol for tracking pro-

decentralized proximity to preserve privacy.

6. Responsibility and obligations

Radar COVID is offered with the best efforts, since its quality

and availability can be affected by multiple factors unrelated to the TITU-

LAR such as, among others, the volume of USERS in the geographical location

of the USER, limitations or restrictions of third-party networks operating

tors or the compatibility of the device and operating system used by the

USERNAME. Likewise, the USERS accept that the service can be seen in-

interrupted when necessary for maintenance work.

For all these reasons, the HOLDER will not be responsible for problems of access or

availability of Radar COVID and/or its services, nor of the damages that may be

could be caused by it, when they come from factors outside their scope

of control. Likewise, the HOLDER is not responsible for the following

facts, or failures, incompatibilities and/or damage to your terminals or devices.

vos that, where appropriate, could be derived from the download and/or use of the Application.

tion:

• Updating, accuracy, exhaustiveness, relevance, timeliness and reliability.

content, whatever the cause and the difficulties or problems

more technical or of another nature in which these facts have their origin.

• The quality, ownership, legitimacy, suitability or relevance of the

materials, and other content.

As a USER of the Application you agree to:

•

Prevent unauthorized third party access to the application

from your device.

• Notify the HOLDER immediately of any indication of the existence

occurrence of a breach of security in the Application, inappropriate use

or prohibited from the services provided from it, or from security failures.

gift of any kind.

• Make good use of the content, information and services provided

from or through the Application, in accordance with the law, good faith and good

generally accepted customs, expressly committing to:

o Refrain from carrying out practices or uses of the services for illicit purposes.

cough, fraudulent, harmful to rights or interests of the HOLDER or third parties,

violators of the rules contained in this document.

o Refrain from carrying out any type of action that could disable,

overload or damage systems, equipment or services of the Application or access

bles directly or indirectly through it.

o Respect the intellectual and industrial property rights of the HOLDER

and third parties about the content, information and services provided from or to

www.aepd.es

sedeagpd.gob.es

C/ Jorge Juan, 6

28001 – Madrid

97/168

through the Application, generally refraining from copying, distributing

buy, reproduce or communicate in any way the same to third parties, unless

give express authorization in writing of the OWNER or of the owners of said

Rights.

o Do not provide false information in the Application, being the only res-

responsible for real and truthful communication.

o Do not impersonate the personality of a third party.

The USER of the Application is solely responsible for the use he decides to make.

czar of Radar COVID services. breach of obligations

as a USER may imply the immediate cancellation of the Application and/or its services.

cios; all this without the right to receive compensation of any kind, and without prejudice

of the corresponding legal actions that the HOLDER may have

place.

The HOLDER will not be responsible in any case for the improper use of

Radar COVID and its contents, the USER being solely responsible

for damages that may arise from misuse of these or from

the infringement of the provisions of these conditions in which it may incu-

laugh The USER undertakes to keep the HOLDER harmless against the

claims or sanctions that you may receive from third parties, whether they are individuals

res or public or private entities, by reason of said infractions, as well as

against damages of all kinds that may be suffered as a consequence

cia of the same.

In any case, the HOLDER reserves, at any time and without

prior notice, the right to modify or delete the content, structure,

design, services and conditions of access and/or use of this Application, provided

that it deems appropriate, provided that said change does not affect the principles and

data protection rights, as well as the right to interpret these

conditions, in as many issues as its application could raise.

Likewise, the reproduction, distribution, transmission, adaptation,

tion or modification, by any means and in any form, of the contents

two of Radar COVID or its courses (texts, designs, graphics, information,

databases, sound and/or image files, logos and other elements of

these sites), unless previously authorized by their legitimate owners.

The above enumeration is merely illustrative in nature and is not, in any way,

case, exclusive or excluding in any of its points. In all suppos-

data, THE HOLDER EXCLUDES ANY RESPONSIBILITY FOR THE DAMAGE

DAMAGES AND DAMAGES OF ANY NATURE ARISING DIRECTLY

OR INDIRECTLY OF THE SAME AND OF ANY OTHER NOT

SPECIFICATIONS OF ANALOGUES CHARACTERISTICS.

The HOLDER DOES NOT OFFER ANY WARRANTY, EXPRESS, IMPLIED, LEGAL

GAL OR VOLUNTEER.

THE HOLDER EXPRESSLY EXCLUDES ALL IMPLIED WARRANTIES

TAS, INCLUDING, WITHOUT LIMITATION, BUT NOT LIMITATION,

ANY IMPLIED WARRANTY OR COVERAGE OF HIDDEN DEFECTS

TOS, MERCHANTABILITY, SATISFACTORY QUALITY, TITLE, SUITABILITY

OF THE PRODUCT FOR A PARTICULAR PURPOSE AND ANY

WARRANTY OR CONDITION OF NON-INFRINGEMENT. THIS EXCLUSION OF

LIABILITY SHALL ONLY APPLY TO THE EXTENT PERMITTED BY

THE APPLICABLE IMPERATIVE LAW.

7. Links

Radar COVID may include within its content links to sites belonging to

owned and/or managed by third parties in order to facilitate access to information

training and services available through the Internet.

The HOLDER does not assume any responsibility derived from the existence of

links between the contents of Radar COVID and contents located outside

the same or any other mention of content external to this site, ex-

accepting those responsibilities established in the protection regulations

data tion. Such links or mentions have an exclusive purpose

informative and, in no case, imply the support, approval, commercialization

or any relationship between the HOLDER and the persons or entities that are the authors and/or manage-

owners of such content or owners of the sites where they are found, nor

any guarantee of the OWNER for the proper functioning of the sites or content

linked nests.

In this sense, the USER undertakes to use the utmost diligence and prudence

in the case of accessing or using content or services of the sites to which

Access by virtue of the aforementioned links.

8. Hyperlinks

Reproduction of COVID Radar pages via hyperlinks is not supported.

ce from another mobile application or web page, allowing exclusively the

access from the application.

In no case may it be implied that the OWNER authorizes the hyperlink

ce or that has supervised or assumed in any way the services or content

two offered by the website from which the hyperlink is produced.

False, incorrect or inappropriate statements or references may not be made.

data on the pages and services of the HOLDER.

The creation of any type of browser, software or software is explicitly prohibited.

ma, “browser” or “border environment” on the Radar COVID pages.

Content contrary to the rights of third parties may not be included, nor may

contrary to morality and accepted good customs, nor content or information

illicit actions, on the web page from which the hyperlink is established.

The existence of a hyperlink between a web page and the COVID Radar does not im-

implies the existence of relationships between the OWNER and the owner of that page.

na, nor the acceptance and approval of its contents and services.

9. Applicable law and jurisdiction

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

These conditions of use will be governed and interpreted in each and every

one of its extremes by Spanish Law. In those cases in which the norm

current policy does not provide for the obligation to submit to a jurisdiction or legislation

determined, the HOLDER and the USERS, waiving any other jurisdiction

that may correspond to them, submit to the courts and tribunals of Madrid

capital (Spain).

10. Corporate information and contact

Address: Calle de Manuel Cortina, 2, 28010 Madrid

The support to the USER in case of incidents and/or claims will be

fully online and attended to

brevity:

support.radarcovid@covid19.gob.es

the biggest

TWENTY SIXTH: The technical document "Implementation procedure

of the Radar COVID App as a complement to manual identification systems

of contacts" in its version of August 14, 2020, coordinated by:

- Coordination Center for Health Alerts and Emergencies.

- General Directorate of Public Health, Quality and Innovation.

TWENTY-SEVENTH: On August 19, 2020, the Interterritorial Council of the

National Health System, signs an "Agreement for the use of the application "Radar COVID",

in the testing phase, by the Autonomous Communities and Autonomous Cities

more" which says:

To contribute to these tasks of active search for close contacts of ca-

sos confirmed, from the Secretary of State for Digitization and Intelligence

Artificial (SEDIA), has been developed, in coordination with other members of the

EU and the eHealth network, a digital tool to complement the tasks of

manual search of contacts that carry out the corresponding services

of the autonomous communities and cities. (…)

During the month of July 2020, the General Secretariat of Digital Administration,

governing body dependent on the Secretary of State for Digitization and Intelligence

Artificial Agency, successfully carried out a pilot project to test the func-

operation of this application on the island of La Gomera. (…)

This Temporary Agreement allows you to establish the terms of use by

the autonomous communities and cities of the "RADAR COVID" application during

said testing phase, until the date of full operation of the same, which will be

will occur by adhering to the application through the appropriate conventions.

Bilateral children of the Secretary of State for Digitization and Artificial Intelligence

with the different autonomous communities and cities.

In point 5 it says:

5. In relation to the processing of personal data, and in application

of the regime provided for in Regulation (EU) 2016/679 of the European Parliament and

of the Council of April 27, 2016, regarding the protection of natural persons

with regard to the processing of personal data and the free movement of

these data and by which Directive 95/46/CE is repealed, during the validity of

this Agreement, the data controller will be the Ministry of Health and, in

their respective territory, each of the autonomous communities and cities that

are incorporated during the testing phase to the use of the application, ostensibly

fully exploiting its competencies in health matters. The handler-

will be, in both cases, the Secretary of State for Digitization and Intelligence.

Artificial agency.

TWENTY-EIGHTH: At the national level, the commissioning of the Radar application

COVID occurs on August 19, 2020.

TWENTY-NINTH: There is a first version of the document "Analysis of Risks

Covid19 Radar Service" dated August 2020, prepared by MINTSAIT an

INDRA COMPANY.

THIRTIETH: In the final version of the "Privacy Policy of the Application

Radar COVID" published in October 2020, contains the following information:

PRIVACY POLICY OF THE APP Radar COVID

Please read this privacy policy for users of the website carefully.

mobile application "Radar COVID" (or the "Application"), where you can find

all information about the data we use, how we use it and what it contains

troll you have on them.

IMPORTANT ANNOUNCEMENT:

The USER is warned that the use of the Application DOES NOT CONSTITUTE

YOU DO NOT UNDER ANY CIRCUMSTANCES A MEDICAL DIAGNOSIS SERVICE,

EMERGENCY CARE OR TREATMENT PRESCRIPTION

PHARMACOLOGICAL, since the use of the Application could not in any way

replace the personal face-to-face consultation with a medical professional

duly qualified.

1. What is COVID Radar?

Radar COVID is an application for mobile devices of alert of conta-

SARS-CoV-2 virus, whose HOLDER is the General Secretariat of Admi-

Digital Administration, dependent on the Secretary of State for Digitization and

Artificial Intelligence of the Ministry of Economic Affairs and Transformation

Digital.

Thanks to Radar COVID, those users who have downloaded the app-

tion and accept its use will receive a notification in the event that in the fourteen

days prior to that notification have been exposed to an epidemic contact

myological (less than two meters and more than 15 minutes) with another user (all

anonymous) who has declared in the application to have given a result

do positive in the COVID 19 test (prior accreditation of the authorities

sanitary). The application will inform you exclusively about the day (within

those previous fourteen) in which exposure to contact

but not about the identity of the user to whom it has been exposed (information

tion impossible as it is an application that does not request, use or store data from

personal character of the users) nor the identification of the device of this, nor

about the time or place where the exposure occurred.

Once a notification is received, the application will provide the exposed user with information

tion for the adoption of preventive and assistance measures, to contribute

thus to contain the spread of the virus.

The success of the application as a tool that contributes to the containment of

spread is directly linked to users being aware,

and act accordingly, that, despite communicating to the application

that a positive result has been obtained in the COVID 19 test (prior

accreditation of the health authorities) is voluntary, not communicating it and

being a mere receiver of information from third-party users makes the application

tion loses its preventive usefulness not only for other users but for the

rest of the general population. The completely anonymous character should

encourage, without a doubt, the exercise of this responsible action.

2. How does the app work?

Once you have downloaded the application, accept the conditions of

use and privacy policy and start using it, your mobile device generates

each day will generate a random identifier called a “temporary exposure key”.

ral” with a size of 16 characters (16 bytes or 128 bits) that will be used to derive

var “Bluetooth ephemeral identifiers” that are exchanged with other

nearby mobile phones that also have the Radar application downloaded.

Give COVID and activated your Bluetooth.

“Bluetooth ephemeral identifiers” are random codes with a size

16 characters (16 bytes, or 128 bits), which are generated by your mobile phone

every 10-20 minutes, starting from the daily “temporary exposure key”. These

codes do not contain personal information, which allows to identify the phone

mobile or the user thereof. These “Bluetooth ephemeral identifiers” are

transmitted by your mobile phone several times per second to nearby devices.

gray, accessible via Bluetooth Low Energy (BLE, Bluetooth Low

Energy), producing an exchange of random codes between devices

so that they can be stored by nearby phones that have downloaded

I win the app. Similarly, every five minutes, your mobile phone is-

will listen for ephemeral Bluetooth identifiers that are broadcast by other

mobile phones that have the application and will store them to determine if

you have been with another user infected by COVID-19 over the last

14 days after you have reported a positive.

Your phone stores the temporary exposure keys that you have generated in

the last 14 days. Remember that these keys are randomly generated and not

They serve to identify your mobile phone or its USER.

If you have received a positive diagnosis for COVID-19, you can enter volunteers

maryly in the application the "single-use confirmation code" that you

will facilitate your Public Health Service and that will be validated on the server of the

SGAD. At that time, the application will ask for your consent to send

throw to our server up to a maximum of the last 14 exposure keys

temporarily stored on your phone, therefore, only if you lend it, they are sent

will be sent to the SGAD server which, after verifying the accuracy of the code,

will serve to compose a daily list of temporary exhibition keys of

people infected by COVID-19 that are downloaded daily from

the server by all the Radar COVID applications that are running

I lie.

The information in these listings is used so that on your own phone you can

check if you have had close contact (less than two meters and more than 15

minutes) with people who have reported a COVID-19 infection, without identity.

tify neither the person, nor the place of exposure, nor the mobile device, nor any-

any personal information about you or the other person. That is, the application downloads

voluntarily shared temporary exposure keys periodically

by users diagnosed by COVID-19 of the server, to compare them

with the random codes recorded in the previous days as a result of

contacts with other users. If a match is found, the application

runs an algorithm on the device that, based on the duration and distance

estimated contact, and according to the criteria established by the

health authorities, evaluates the risk of exposure to the SARS-CoV-2 virus and

in its case, it shows a notification warning the user of the risk contact.

rio, informing him of the date of the same and inviting him to self-isolate and contact

deal with the health authorities.

These keys sent to the server do not allow the direct identification of the

users and are necessary to guarantee the correct functioning of the system.

risk contacts alert ma.

3. Who is responsible for processing your data as a user?

from “COVID Radar”?

This application is responsible for processing both the Ministry of

Health, as well as the Autonomous Communities. Likewise, the General Secretariat

The General Director of Digital Administration acts as the person in charge of the treatment.

At the national level, the person responsible for processing your data as a user of

“COVID Radar” is:

As part of the COVID-19 contagion alert system, data will be processed

the following data for users who have tested positive for COVID-19

for the purposes specified below:

Name: Ministry of Health.

Address: Paseo del Prado 18-20, 28014 Madrid

The General Secretariat of Digital Administration, as the owner of the application

cation and based on the order of the treatment entrusted by the Ministry of

Health, will carry out the following treatment operations:

Generation of codes for the communication of positives in the Ra-

give COVID.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Reception of the information sent by users when they communicate a

positive. This information includes:

Daily exposure keys up to a maximum of 14 days. the exact number

of communicated codes will depend on the date of onset of symptoms or date of

diagnosis that is reported in the application.

The preference or not to communicate these daily exposure keys to the node

European framework for interoperability between contact tracing applications.

Composition of an updated list of temporary exhibition keys that

are made available for download by Radar applications.

give COVID.

In relation to the European contact interoperability node (EFGS).

Daily reception of the lists of temporary exhibition keys generated

by the national servers of the Member States adhered, where appropriate, to the

Project.

Daily submission to the EFGS node of a list of temporary exposure keys

submitted by Radar COVID users who have explicitly consented

share this information with the rest of the Member States adhering to the program.

project.

The Autonomous Communities adhered to the use of the application are, likewise,

mo, data controllers, carrying out the following operations

of treatment:

Request to the Radar COVID server to generate confirmation codes

of positive.

Delivery of these codes to people diagnosed positive by tests

PCR.

The person in charge of the treatment and owner of the application is the General Secretariat

of Digital Administration, the governing body of the Secretary of State for Digital

and Artificial Intelligence of the Ministry of Economic Affairs and Trans-

Digital training, under the Agreement between the Ministry of Economic Affairs

and Digital Transformation (Secretariat of State for Digitization and Inteli-

Artificial Agency) and the Ministry of Health about the application "Radar CO-

VINE".

4. What data do we process about you?

The data handled by the application does not allow the direct identification of the

user or your device, and are only those necessary for the sole purpose of information

Mars that you have been exposed to a situation of risk of contagion by the

COVID-19, as well as to facilitate the possible adoption of preventive measures

and assistance.

In no case will the movements of USERS be tracked, excluding

thus any form of geolocation.

The IP address of the USERS will not be stored or processed.

Positive confirmation codes will not be stored together with other data.

users' personal cough.

As part of the COVID-19 risk contact alert system,

will process the following data for users who have tested positive for

COVID-19 for the purposes specified below:

The temporary exposure keys with which the user's device has generated

generated the random codes sent (Bluetooth ephemeral identifiers), to

devices with which the user has come into contact, up to a maximum

mo of the previous 14 days. These keys have nothing to do with the identity

entity of the USER, and are uploaded to the server so that they can be downloaded

by Radar COVID apps held by other users. With these keys,

through processing that takes place in the mobile phone unintentionally.

centralized, the USER can be warned about the risk of contagion by ha-

have been in recent contact with a person who has been diagnosed

by COVID-19, without the application being able to derive your identity or the place where

the contact took place.

A 12-digit one-time confirmation code provided by the authorities

health information to the USER in case of a positive test for COVID-19. East

code must be entered below by the user in the application to

allow the voluntary upload to the server of temporary exposure keys.

The user's consent, if applicable, for the remission of exposure keys

temporary assignment to the European tracing application interoperability node

of contacts.

The notice of notification of exposure, in order to collect statistics

anonymous and aggregate of the volume of notifications produced by the system to

through contact tracing. These data allow estimating how many users

have been alerted by the Application, of a potential risk of infection, without being able to

to trace your identity.

All information will be collected for strictly public interest purposes.

the field of public health, and in the event of a health emergency, decrees

tada, in order to protect and safeguard an interest essential to the lives of the

people, in the terms described in this privacy policy, and attending

to articles 6.1.a), 9.2.a), 6.1.c), 6.1.d), 6.1.e), 9.2.c), 9.2.h) and 9.2.i)

The applicable legislation is listed below:

Regulation (EU) 2016/679, of April 27, 2016, regarding the protection of

natural persons with regard to the processing of personal data and

the free movement of these data and repealing Directive 95/46/EC

(General Data Protection Regulation).

Organic Law 3/2018, of December 5, on the Protection of Personal Data and

guarantee of digital rights.

Organic Law 3/1986, of April 14, on Special Measures in the Matter of

www.aepd.es

sedeagpd.gob.es

C/ Jorge Juan, 6

28001 – Madrid

105/168

Public health.

Law 33/2011, of October 4, General Public Health.

Law 14/1986, of April 25, General Health.

Royal Decree Law 21/2020, of June 9, on urgent prevention measures,

containment and coordination to deal with the health crisis caused by

the COVID-19.

Agreement of October 9, 2020, between the Ministry of Economic Affairs and

Digital Transformation (Secretariat of State for Digitization and Intelligence

Artificial) and the Ministry of Health about the “Radar COVID” application.

5. How do we obtain and where does your data come from?

The positive confirmation code for COVID-19 provided by the Service

Health Public. This will allow the upload to the server of the exposure keys.

temporary tion with which the user's device has generated the codes

random sent (Bluetooth ephemeral identifiers) to devices with

which the user has come into contact, up to a maximum of 14 days before.

beef. These keys are only uploaded to the server with the explicit consent

I quote and unequivocal of the USER, having entered a confirmation code

positive for COVID-19.

The exposure notification notice is provided by the application in a

anonymous for the purpose of composing an aggregate statistic of the volume of

users who have been notified.

6. For what and why do we use your data?

The collection, storage, modification, structuring and, where appropriate, elimination

nation, of the data generated, will constitute treatment operations carried out

carried out by the Holder, in order to guarantee the correct functioning

use of the App, maintain the service provision relationship with the User.

rio, and for the management, administration, information, provision and improvement of the service

vice.

The information and data collected through the Application will be treated with

purposes strictly of public interest in the field of public health, given the

current health emergency situation as a result of the pandemic

of COVID-19 and the need for its control and spread, as well as to gain

guarantee your vital interests or those of third parties, in accordance with the regulations

current data protection.

For this purpose, we use your data to provide you with the "Radar COVID" service and

so that you can make use of its functionalities in accordance with its conditions.

tions of use. In accordance with the General Regulation for the Protection of

Data (RGPD) as well as any applicable national legislation, the

General Secretariat of Digital Administration will treat all the data generated

while using the App for the following purposes:

Offer you information on contacts considered to be at risk of exposure to

the COVID-19.

Provide you with practical advice and recommendations for actions to follow

According to situations of risk in the face of quarantine or self-quarantine,

I had

The data will always and only be used anonymously for statistical purposes.

ethical and epidemiological.

This treatment will be carried out through the alert functionality of

contagion that allows to identify situations of risk for having been in

close contact with users of the application who are

infected by COVID-19. In this way you will be informed of the measures

which should be adopted later.

7. How long do we keep your data?

Temporary Exposure Keys and Ephemeral Bluetooth Identifiers

are stored on the device for a period of 14 days, after the

which are eliminated.

Likewise, the temporary exhibition keys that have been communicated to the

server by USERS diagnosed as positive for COVID-19 also

They will also be removed from the server after 14 days.

In any case, neither the temporary exposure keys nor the ephemeral identifiers

Bluetooth ros contain personal data and do not allow identifier

users' mobile phones.

The exposure notification notice is added in the daily notices indicator.

communicated rivers, being discarded for any other use.

8. Who has access to your data?

The data managed by the mobile application (daily exposure keys

temporary and ephemeral Bluetooth identifiers) are stored only in the

user's device in order to be able to make calculations and notify the USER

RIO about your risk of exposure to COVID-19.

Only in the case of reporting a positive diagnosis for COVID-19, the keys

of temporary exposure of the last 14 days generated on the device, and

under the explicit and unequivocal consent of the USER, are uploaded to the ser-

viewer for dissemination to all USERS of this system.

These keys have nothing to do with the identity of the devices

mobile phones or with personal data of the USERS of the Application.

The communicated exposure notification notices are only used for the

generation of aggregated and anonymous statistical data.

9. What are your rights and how can you control your data?

The current regulations grant you a series of rights in relation to the data

and information we process about you. Specifically, access rights,

rectification, deletion, limitation and opposition.

You can check the scope and full details of them on the page

website of the Spanish Data Protection Agency (AEPD) here.

In general, you can exercise all these rights at any time.

ment and for free. You can contact the Treatment Managers

electronically, either the Ministry of Health or the Autonomous Community of residence.

dence. In the case of the Ministry of Health, you can do it through

this form, or in person through the assistance office network

regarding records using this application form (editable version and

printable).

Likewise, you have the right to file a claim at all times.

tion before the Spanish Data Protection Agency.

10. How do we protect your data?

Those Responsible, as well as the SGAD in charge of processing

guarantee the security, secrecy and confidentiality of your data,

communications and personal information and have adopted the most demanding and

extensive security measures and technical means to prevent loss, misuse

or its access without your authorization. The security measures implemented are co-

correspond to those provided for in Annex II (Security measures) of the Real

Decree 3/2010, of January 8, which regulates the National Scheme of

Security in the field of Electronic Administration.

Finally, we inform you that both the storage and the rest of the

Non-personal data processing activities used will always be

located within the European Union.

11. What do you have to take into account especially when using "Radar COVID"?

You must take into account certain aspects related to the minimum age of

use of the Application, the quality of the data you provide us, as well

such as uninstalling the Application on your mobile device.

Minimum age of use: to be able to use "Radar COVID" you have to be

over 18 years of age or have the authorization of your parents and/or legal guardians.

them. Therefore, by registering in the Application, you guarantee the Owner that you are

older than that age or, otherwise, that you have the aforementioned autho-

torization

Quality of the data you provide us: the information you provide us in

the use of the Application services must always be real, truthful and es-

updated tar.

App Uninstall: In general, you can uninstall the app in

your device at any time. This process removes from your mobile phone

the history of codes received from other mobile phones for the functions

close contact alerts.

12. Transfer of data to countries of the European Union

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Radar COVID participates in the application integration platform of the

European Union, so that the positive keys will be shared with third parties

EU countries and vice versa.

When the user's device downloads the positive keys to analyze

possible close contacts, it will also download the positive keys of third parties.

ros countries adhering to the European project.

This will make it possible to identify possible close contacts whether the user has been

been visiting any of these countries as if you have been in close contact

with a visitor from these countries.

When the user enters a positive diagnostic confirmation code

by COVID-19, the user's free, specific, independent consent will be requested.

formed and unambiguous to share your infected keys with third countries

through the European interoperability platform facilitating direct tracking

gital from possible close contacts. The communication of your infected keys

given to the network of European countries adhering to this project is completely

volunteer.

No data transfers will be made outside the European Union

13. Cookie Policy

We only use technical cookies that allow the user to navigate and

the use of the different options or services offered in the Application

tion, such as accessing restricted access areas or using electronic elements.

safety measures during navigation.

I have read the document PRIVACY POLICY OF THE APPLICATION "Ra-

give COVID."

THIRTY FIRST: In the final version of the "Terms of Use of Radar

COVID" contains the following information:

Radar COVID TERMS OF USE

BY DOWNLOADING AND USING THE “Radar COVID” MOBILE APPLICATION MANI-

PARTIES THAT YOU HAVE READ AND ACCEPT THESE TERMS OF USE AND

THE PRIVACY POLICY. HERE IS ALL THE INFORMATION

REGARDING YOUR RIGHTS AND OBLIGATIONS AS A USER OF

THIS APPLICATION.

IMPORTANT ANNOUNCEMENT:

The USER is warned that the use of the Application DOES NOT CONSTITUTE

YOU DO NOT UNDER ANY CIRCUMSTANCES A MEDICAL DIAGNOSIS SERVICE,

EMERGENCY CARE OR TREATMENT PRESCRIPTION

PHARMACOLOGICAL, since the use of the Application could not in any way

replace the personal face-to-face consultation with a medical professional

duly qualified.

1. What is COVID Radar

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

109/168

Radar COVID is an application that promotes public health through a

alert system for risk contacts in relation to COVID-19, putting

available to USERS (hereinafter, individually, the "USER",

and jointly the "USERS"), the possibility of browsing the Application,

accessing the contents and services of Radar COVID, in accordance with the

these TERMS OF USE.

Radar COVID detects the strength of Bluetooth signals exchanged between

devices that have this active application, through the use of identifiers
ephemeral random factors, unrelated to the identity of the phone.
mobile phone employee or the USER. The device of each USER downloaded
Periodically generate the Bluetooth keys of all the USERS of the application.
tion that they have reported through the same that they have been diagnosed
COVID-19 (prior accreditation of the health authorities), proceeding to
determine if the USER has established risk contact with any of the
them, verified by the Bluetooth signals exchanged. If this is the case, the
cation notifies you of this fact, so that you can take action, and contribute
Build in this way to prevent the virus from spreading.
Radar COVID in its architecture uses the Exposure Notification System
tions (SNE) provided by Apple and Google, and developed from the
DP-3T decentralized proximity tracking protocol to preserve the
privacy.
2. Use of COVID Radar
To use the Radar COVID services, it is a necessary requirement that
the USER authorizes the activation of the Bluetooth communications system of
low energy (BLE, Bluetooth Low Energy) by the Application, after the
download of it.
The USER accepts without reservation the content of these CONDITIONS
OF USE. Consequently, the USER must carefully read the same
more before accessing and using any Radar COVID service
under your entire responsibility.
IMPORTANT NOTICE: The use of the Application is free, free and voluntary.
would for all citizens. To use Radar COVID it is not necessary to be-
be registered, nor provide any personal, identifying or non-identifying data.

By activating the application, the USER accepts:

a) sending anonymously emitted Bluetooth signals by your device;

b) the reception and storage of Bluetooth signals from applications

compatible with Radar COVID, which are kept anonymous and decentralized

stored on USERS' devices for a period not exceeding 14

days;

c) the information offered to the USER about the possible risk of contagion, without

that at no time personal data of any kind is referred.

d) receive positive codes from third countries of the European Union through

the European Union Interoperability Platform (EFGS);

e) under explicit consent, the sending of positive keys that will be

games with third countries of the European Union through the platform of

interoperability of the European Union (EFGS).

The USER can voluntarily inform the application of a result

positive in your COVID-19 tests using the confirmation code of

a single use facilitated by the health authorities. The validity of this code

will be checked by the application to ensure the correct operation of Ra-

give COVID. The USER will report the results of their tests and will be

will request the express and unequivocal consent to share the generated keys.

generated daily on your device, and corresponding to the last 14

days. These keys are communicated to a server that will make them available

of the Radar COVID suite of applications for download. The keys with

communications have nothing to do with the identification of the device or the

USERNAME.

3. Security and privacy

The security measures implemented correspond to those provided for in the

Annex II (Security measures) of Royal Decree 3/2010, of January 8, by the

which regulates the National Security Scheme in the field of the Administration

Electronic tration.

We inform you that your data will be treated in accordance with the provisions of the

Privacy Policy of the Application, the full content of which can be found

See the following link: Privacy Policy.

All information will be treated strictly for purposes of public interest in the

field of public health, and in view of the health emergency situation decreed

in order to protect and safeguard an interest essential to the lives of persons

sonas, in the terms described in the privacy policy.

The information on the activity of the USERS is anonymous and in no way

At this time, USERS will not be required to provide any personal data. At all times, the

USER can disable the Bluetooth contact tracing system in the

application, as well as uninstall the Application.

4. Change of service and termination

Radar COVID is always trying to improve the service and seeks to offer func-

useful additional features for the USER, always bearing in mind the

preservation of public health. This means that we can add new

features or enhancements, as well as remove some of the features. If you are new

These functions or improvements materially affect the rights and obligations

of the USER, will be informed through the Application so that it adopts the

timely decisions about continued use.

The USER can stop using the application at any time and for

any reason, by uninstalling it from your device.

5. App Holder

The General Secretariat of Digital Administration (SGAD), dependent on the Sec-

Secretary of State for Digitization and Artificial Intelligence of the Ministry of

Economic Affairs and Digital Transformation, is the OWNER body of the

app.

6. Responsibility and obligations

Radar COVID is offered with the best efforts, since its quality

and availability can be affected by multiple factors unrelated to the TITU-

LAR such as, among others, the volume of other USERS in the location

geographic location of the USER, limitations or restrictions of third-party networks

operators or the compatibility of the device and operating system used by

the user. Likewise, the USERS accept that the service can be seen

interrupted when necessary for maintenance work.

For all these reasons, the HOLDER will not be responsible for problems of access or

availability of Radar COVID and/or its services, nor of the damages that

could cause for it, when they come from factors outside their scope.

control guy.

Likewise, the HOLDER is not responsible for the following facts, nor

of failures, incompatibilities and/or damages of your terminals or devices that, in

your case, could be derived from the download and/or use of the Application:

Updating, accuracy, completeness, relevance, timeliness and reliability of

its contents, whatever the cause and the difficulties or technical problems

unique or of another nature in which these facts have their origin.

The quality, ownership, legitimacy, adequacy or relevance of the materials,

and other content.

As a USER of the Application you agree to:

Prevent unauthorized third party access to the application from your

device.

Notify the HOLDER immediately of any indication of the existence

of a breach of security in the Application, inappropriate use or

prohibited from the services provided from it, or security flaws

of any kind.

Make good use of the content, information and services provided from or to

through the Application, in accordance with the law, good faith and good customs.

generally accepted names, expressly committing to:

Refrain from carrying out practices or uses of the services for illicit purposes, fraud,

dulent, harmful to the rights or interests of the HOLDER or third parties, infringing

res of the rules contained in this document.

Refrain from performing any type of action that could render useless, overload

garnish or damage systems, equipment or services of the Application or directly accessible

or indirectly through it.

Respect the intellectual and industrial property rights of the HOLDER and of

third parties about the content, information and services provided from or through

through the Application, generally refraining from copying, distributing,

reproduce or communicate in any way the same to third parties, if there is no

express written authorization of the HOLDER or of the holders of said rights.

rights.

Do not provide false information in the Application, being solely responsible

real and truthful communication.

Do not impersonate the personality of a third party.

The USER of the Application is solely responsible for the use he decides to make.

czar of Radar COVID services.

The HOLDER will not be responsible in any case for the improper use of

Radar COVID and its contents, the USER being solely responsible

for damages that may arise from misuse of these or from

the infringement of the provisions of these conditions in which it may incu-

laugh The USER undertakes to keep the HOLDER harmless against the

claims or sanctions that you may receive from third parties, whether they are private

res or public or private entities, by reason of said infractions, as well as

against damages of all kinds that may be suffered as a consequence

cia of the same.

In any case, the HOLDER reserves, at any time and without

prior notice, the right to modify or delete the content, structure,

design, services and conditions of access and/or use of this Application, provided

that said change does not affect the principles and rights of data protection,

as well as the right to interpret these conditions, in all questions

nes could raise your application.

Likewise, the reproduction, distribution, transmission, adaptation,

tion or modification, by any means and in any form, of the contents

two of Radar COVID or its courses (texts, designs, graphics, information,

databases, sound and/or image files, logos and other elements of

these sites), except as permitted by the open source release license

under which the system has been published.

The above enumeration is merely illustrative in nature and is not, in any way,

case, exclusive or excluding in any of its points. In all suppos-

data, THE HOLDER EXCLUDES ANY RESPONSIBILITY FOR THE DAMAGE

DAMAGES AND DAMAGES OF ANY NATURE ARISING DIRECTLY

OR INDIRECTLY OF THE SAME AND OF ANY OTHER NOT

SPECIFICATIONS OF ANALOGUES CHARACTERISTICS.

The HOLDER DOES NOT OFFER ANY WARRANTY, EXPRESS, IMPLIED, LEGAL

GAL OR VOLUNTEER.

THE HOLDER EXPRESSLY EXCLUDES ALL IMPLIED WARRANTIES

TAS, INCLUDING, WITHOUT LIMITATION, BUT NOT LIMITATION,

ANY IMPLIED WARRANTY OR COVERAGE OF HIDDEN DEFECTS

TOS, MERCHANTABILITY, SATISFACTORY QUALITY, TITLE, SUITABILITY

OF THE PRODUCT FOR A PARTICULAR PURPOSE AND ANY

WARRANTY OR CONDITION OF NON-INFRINGEMENT. THIS EXCLUSION OF

LIABILITY SHALL ONLY APPLY TO THE EXTENT PERMITTED BY

THE APPLICABLE IMPERATIVE LAW.

7. Links

Radar COVID may include within its content links to sites belonging to

owned and/or managed by third parties in order to facilitate access to information

training and services available through the Internet.

The HOLDER does not assume any responsibility derived from the existence of

links between the contents of Radar COVID and contents located outside

the same or any other mention of external content, except

those responsibilities established in the data protection regulations.

cough. Such links or mentions have an exclusively informative purpose.

and, in no case, imply the support, approval, commercialization or relationship

between the HOLDER and the persons or entities that are authors and/or managers of

such contents or owners of the sites where they are found, nor any guarantee

of the HOLDER for the proper functioning of the sites or linked content.

ted.

In this sense, the USER undertakes to use the utmost diligence and prudence

in the case of accessing or using content or services of the sites to which

Access by virtue of the aforementioned links.

8. Hyperlinks

Reproduction of COVID Radar pages via hyperlinks is not supported.

ce from another mobile application or web page, allowing exclusively the

access from the application.

In no case may it be implied that the OWNER authorizes the hyperlink

ce or that has supervised or assumed in any way the services or content

two offered by the website from which the hyperlink is produced.

False, incorrect or inappropriate statements or references may not be made.

data on the pages and services of the HOLDER.

The creation of any type of browser, software or software is explicitly prohibited.

ma, “browser” or “border environment” on the Radar COVID pages.

Content contrary to the rights of third parties may not be included, nor may

contrary to morality and accepted good customs, nor content or information

illicit actions, on the web page from which the hyperlink is established.

The existence of a hyperlink between a web page and the COVID Radar does not im-

implies the existence of relationships between the OWNER and the owner of that page.

na, nor the acceptance and approval of its contents and services.

9. Applicable law and jurisdiction

These conditions of use will be governed and interpreted in each and every

one of its extremes by Spanish legislation. In those cases where

current regulations do not provide for the obligation to submit to a jurisdiction or legislation

determined, the HOLDER and the USERS, waiving any other

jurisdiction that may correspond to them, submit to the courts and tribunals of

Madrid capital (Spain).

10. Corporate information and contact

Address: Calle de Manuel Cortina, 2, 28010 Madrid

THIRTY-SECOND: On September 9, 2020, the METD publishes this

Press release:

“The RadarCOVID mobile application completes its implementation in thirteen communities

autonomous des, which cover 70% of the population, and releases its code. (…)

In the absence of that necessary integration, the application is up and running on

the entire national territory since last August. This implies that the

minal already stores the anonymous identifiers of the other terminals with which

that you have been in risky contact during the last seven days.

For this reason, and although the technical implementation is in process in some communities,

autonomous entities, it is useful to have the application already installed so that this process of

registration is taking place and to be able to be protected from the first moment.

to which it starts up. More than 3.7 million users have downloaded

and to the application, protecting yourself and those around you against po-

possible chains of contagion.

code release

In addition, one of the commitments acquired with the

start of application development: the release of its code.

This is an exercise in transparency so that the operation of the application

tion can be audited openly and directly by the public. (…)

With the intention of publicizing the operation of the application and resolving the

doubts and issues that citizens share through social networks, the

Secretary of State for Digitization and IA has launched two separate accounts

specific to the application. Thus, from the @AppRadarCOVID account, available

both on Twitter and Instagram, timely information will be shared about

about the news regarding the app and will answer the most frequently asked questions.

tell me to get citizenship."

THIRTY-THIRD: The technical document "Implementation procedure-

tion of the Radar COVID App as a complement to manual identification systems

cation of contacts” in its version of September 15, 2020, coordinated by:

- Coordination Center for Health Alerts and Emergencies.

- General Directorate of Public Health, Quality and Innovation.

THIRTY-FOURTH: There is a draft document of "Questions and answers

about the Radar COVID-19 contact tracing application” that contains the image

institutional gene of the MSND and SEDIA, dated 09.15.2020, and indicates the following information:

training:

How is my privacy protected?

Throughout the design and development process of Radar COVID, the protection

of your privacy has been a priority.

These are some of the measures with which Radar COVID protects your data:

• The application does not collect any data that allows you to trace your identity. By

example, it will not ask you and will not be able to know your name, surnames, address

tion, phone number or email address.

• The app cannot determine where a contact occurred

or who was present.

• The application does not collect any geolocation data, including that of the

GPS system. In addition, it does not track your movements either.

tions.

• The Bluetooth Low Energy code that is transmitted through the Bluetooth

The application is generated randomly and does not contain any information.

mation about your mobile device or about you. Also, this code changes

several times every hour to further protect your privacy.

• The data stored on your mobile phone is encrypted.

• The connections between the application and the server are encrypted.

• All data, including data stored on your device (in-codes)

exchanged with other mobile phones) and those collected on the server

(from mobile phones where a diagnosis has been reported

positive) are eliminated after 14 days.

• The health system does not save the positive codes generated associa-

linked to a positive diagnosis neither in the clinical history nor in another location.

unto

• No data stored on mobile phones or on the server allows the

identification neither of the mobile device nor of its user.

• Radar COVID does not handle information that can be sold or used

for any commercial purpose, including profiling for

advertising. This project is not for profit, being created

exclusively to help fight the epidemic.

THIRTY-FIFTH: There are two versions of the Impact Assessment:

In the first version, dated September 2020, it says:

“For this reason, and by virtue of the provisions of article 27.3, those responsible for the traffic-

will be the autonomous communities, the cities of Ceuta and Melilla and the

Ministry of Health, within the scope of their respective powers, which guarantees

will enforce the application of mandatory security measures resulting from the co-

corresponding risk analysis, taking into account that the treatments affect

to COVID Radar 10 special categories of data and that said treatments se-

will be carried out by public administrations obliged to comply with the Scheme

ma National Security.

In this case, the owner of the application is the General Secretariat of Administration

Digital under the Ministry of Economic Affairs and Digital Transformation.

such, that it is also constituted as Responsible for the Treatment".

In the second version, it says:

"For this reason, and by virtue of the provisions of article 27.3, those responsible for the traffic-

will be the autonomous communities, the cities of Ceuta and Melilla and the

Ministry of Health, within the scope of their respective powers, which guarantees

will enforce the application of mandatory security measures resulting from the co-

corresponding risk analysis, taking into account that the treatments affect

a Radar COVID 10 special categories of data and that said treatments se-

will be carried out by public administrations obliged to comply with the Scheme

ma National Security.

The data controller is the General Directorate of Public Health, depending

tooth of the Ministry of Health.

The person in charge of treatment is the General Secretariat of Digital Administration,

dependent on the Ministry of Economic Affairs and Digital Transformation, which

has developed the Application."

Likewise, in the first version of the Impact Assessment, it is indicated regarding its

The purpose of this document is to present the results of the

Risk Analysis carried out for the Covid19 Radar Service with respect to the National Scheme

end of Security".

They assert that "The application does not request any personal data, nor does it require

create user (without login or personal data). The application uses anonymous keys and

exchange random identifiers, which are constantly changing. The im-

applied in the application knows the type of information and, most importantly, the

Security policy".

In accordance with the foregoing and the content of this, the impact assessment is limited to

undermine compliance with the ENS, without entering into a possible risk analysis or evalua-

data protection impact tion.

THIRTY-SIX: There is a second version of the document "Analysis of

Radar Service Risks Covid19" dated September 2020, prepared by

MINTSAIT an INDRA COMPANY.

The main objective of Risk Analysis is to determine the level of risk at which

the assets of the Covid19 Radar Service are exposed, taking into account the

threats to which they are exposed and the level of effectiveness of the controls implemented

ted currently to protect them. The Risk Analysis is based on the information

training provided by INDRA's technical managers and those responsible

of the development, start-up and implementation of the Covid19 Radar Application,

those who know the infrastructure and who, therefore, can know the degree of

implementation of each of the security measures in Annex II of the Scheme

National Security. On the other hand, this document has been prepared

with the information collected up to its date of publication, so that, unless otherwise indicated,

express mention, changes made after this date will not be reflected.

two in the same. As mentioned above, the level of risk is

can be classified on a scale from 0 to 10, with 0 being negligible risk and

the value 10 the extremely critical risk. Taking into account this scale, and

taking as metric for the level of risk the highest risk value identified

in an asset, the result of the Risk Analysis determines a Risk Level

Current = {2,6}. Attending to the minimum levels of maturity required by the Es-

burning National Security and taking for the objective risk the same metric

that has been taken for the residual risk, that is, the highest risk value identified

ified in an asset, the objective that is proposed to be achieved in the mitigation process

tion of risks would be established at an Objective Risk Level = {1.8}.

It is recommended to address a set of actions to improve safety measures

currently existing, in order to adjust the level of risk of the Service

Vice Radar Covid19 at a LOW level. These actions have focused on

security measures that can minimize the threats that bring a level

of MEDIUM risk in this Risk Analysis. These actions will allow

reach the level of Objective Risk proposed, since they would increase the degree of

maturity of security measures Mp.info.4 Electronic signature and Op.acc.5 Me-

authentication channels.

The actions proposed in this case are:

- Use qualified certificates for the digital signature used in the ser-

vice of verification of the positives.

- Verify that the hardware cryptographic elements of the AWS Multi-Factor

Authentication (MFA) use algorithms and parameters accredited by the

CCN. In addition, it is recommended to review the access control mechanism to

the PostgreSQL Database to conclude that it meets the requirements

high level

THIRTY-SEVENTH: On October 15, 2020, the BOE published the

“Resolution of October 13, 2020, of the Undersecretary, by which the

Agreement between the Ministry of Economic Affairs and Digital Transformation and the

Ministry of Health, about the application "Radar COVID"”. Dated 10/10/2020

said resolution enters into force.

The Agreement is signed between the Secretary General of Digital Administration, by delegation

ment of SEDIA, and the Secretary General of Digital Health, Information and Innovation

of the National Health System, by delegation of the MSND.

In the "EXPOSE" Sixth says:

“That in application of these principles, since May 2020, the SGAD

has been developing, with the knowledge and agreement of the Ministry of

Health, an application for the traceability of contacts in relation to the pandemic

mine caused by COVID-19 called “Radar COVID. During the month of

July 2020, with the approval of the General Directorate of Public Health, Cali-

and Innovation of the Ministry of Health, the SGAD successfully carried out the pro-

pilot project of the same, whose success guarantees the viability of the proposed solution.

ta for tracing close contacts”

In the "EXPOSE" Ninth it says:

“That, until now, the Ministry of Health has been collaborating with the

SGAD, owner of the “Radar COVID” application, in the functional adjustment processes

end of it from the perspective of public health, coordinating the protocols

epidemiological management of cases detected through the application, and favoring

promoting the progressive incorporation of the autonomous communities and cities into

its use in the testing phase with real data according to the aforementioned Agreement

of August 19, 2020."

The first of the clauses says:

First. Object. It is the object of this Agreement:

a) Delegate to the General Secretariat of Digital Administration (hereinafter,

SGAD) of the Ministry of Economic Affairs and Digital Transformation, all

the skills of design, development, implementation and evolution of the

"Radar COVID" application that correspond to the General Directorate of Health

Digital and Information Systems for the National Health System under

of the provisions of article 8.2.a) of Royal Decree 735/2020, of August 4,

which develops the basic organic structure of the Ministry of Health,

the General Secretariat of Digital Health, Information and Innovation of the System

National Health. The General Secretariat of Digital Health, Information and

Innovation of the National Health System has previously approved the

delegation of all these powers to the SGAD in accordance with

provided for in article 9.1 of Law 40/2015, of October 1.

b) Delegate to the SGAD the competence of the Minister of Health to sign

collaboration agreements with the autonomous communities and cities

for their adherence to the use of the "Radar COVID" application, in accordance

with the provisions of Chapter VI of the Preliminary Title of Law 40/2015, of 1

October, on the Legal Regime of the Public Sector. without prejudice to the support

to facilitate its processing, it will be provided by the General Secretariat of Digital Health,

Information and Innovation of the National Health System.

The second of the clauses says:

Second. Obligations of the parties in relation to the delegation of competence

provisions provided for in letter a) of the first clause:

1. With the signing of this Agreement, in relation to the delegation of competence

provisions provided for in letter a) of the first clause, the SGAD undertakes to

fulfillment of the following obligations:

a) The contracting of evolutionary, corrective, adaptive and perfect maintenance

tive of the "Radar COVID" system from its budget appropriations.

b) The open publication of the source code of the “Radar COVID” system.

c) Support for the operation of the system and the management of the associated infrastructure.

ciada

d) The support and attention to users and autonomous communities and cities in

regarding the technical aspects of this system.

e) Any other obligations necessary for the proper functioning

of the application and, in particular, its integration with the European system of

change of contacts, including the formal application for joining the system.

2. Decisions regarding the evolution of the Application will be made in accordance with

common agreement between the parties.

3. In relation to the delegation of powers provided for in letter a) of the

first clause of this Agreement, correspond to the General Secretariat of

Digital Health, Information and Innovation of the National Health System, in addition to

more than its obligations as Responsible for the processing of character data.

ter staff, and its General Directorate of Digital Health and Information Systems

for the National Health System, the following obligations:

a) Monitoring the design and implementation of the “Radar COVID” system.

b) The reception of the data held by the SGAD (related to

your active download, use, codes used, etc) for proper monitoring

epidemiology of the Pandemic in Spain, as well as its relationship with other countries.

ses europeans

c) The promotion of the necessary measures for its correct application within the

scope of competence of the General Secretariat of Digital Health, Information

and Innovation of the National Health System, as well as the promotion of agreements

two that were necessary to adopt in this regard in the Interterritorial Council of the

National system of health.

d) The analysis of compliance with objectives and, where appropriate, the proposal for re-

formulation of procedures and indicators to adjust them to social needs

briefings.

e) Any other obligations necessary for the proper functioning

of the application.

The third of the clauses in section 1.f) and 2 says:

1.f) The establishment of time limits for the limitation and deletion of information

obtained, including the application logs, as part of the life cycle of the

data, prior approval of the Ministry of Health in its capacity as responsible

ble of the treatment.

2. In the aforementioned collaboration agreements, the Ministry of Health and

the Ministry responsible for health matters in the autonomous community or city.

the tone in question will appear as data controllers

of a personal nature and the SGAD as the data processor, for the purposes

provided for in Regulation (EU) 2016/679 of the European Parliament and of the Con-

Council of April 27, 2016 regarding the protection of natural persons in relation to

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

data and repealing Directive 95/46/EC (General Regulation of

data protection) and in Organic Law 3/2018, of December 5, on Pro-

Protection of Personal Data and guarantee of digital rights and other regulations

application in terms of data protection.

3. In relation to the delegation of powers provided for in letter b) of the

first clause of this Agreement, correspond to the General Secretariat of

Digital Health, Information and Innovation of the National Health System, in its

condition of Responsible for the processing of personal data, give

the necessary indications to the SGAD in its capacity as data processor.

I lie.

Likewise, they correspond to the General Secretariat of Digital Health, Information

and Innovation of the National Health System and its General Directorate of Health

Digital and Information Systems for the National Health System the following

following obligations:

a) Collaboration with the SGAD and the ministries of the communities and citizens

autonomous authorities competent in the matter in all the necessary actions

for the correct implementation and development of the “Radar COVID” system.

b) Ensure the proper functioning of the “Radar COVID” system, in particular

cular in relation to the defense of the rights of the interested parties.

c) The permanent monitoring of the results of the “Radar COVID” system

to transfer them to the health authorities of the different Administrations

Public.

d) The promotion of the necessary measures for its correct development and execution.

tion within the scope of competences of the General Secretariat of Di-

gital, Information and Innovation of the National Health System, as well as the im-

pulse of the agreements that were necessary to adopt in this regard in the Council

Interterritorial of the National Health System.

e) Any other obligations necessary for the successful completion of the application

that can be addressed from the powers of the said General Secretariat.

The tenth clause says:

Tenth. Data protection, security and confidentiality regime.

1. The personal data protection regime in the actions

that are developed in execution of this Agreement will be the one foreseen in the Re-

general data protection regulations and in Organic Law 3/2018, of 5

December, and other applicable regulations on data protection.

2. The parties will ensure compliance with Royal Decree 3/2010, of 8

January, which regulates the National Security Scheme in the field of

Electronic Administration.

3. All information provided by the parties and all information generated

as a consequence of the execution of this Agreement, will have the treatment

confidential, without prejudice to the information that is in the public domain,

being able to be disclosed or facilitated to third parties, nor used for a different purpose

provided in this document, without the unanimous agreement of the parties.

4. The obligation of confidentiality for the parties will be extended indefinitely.

mind even if the Agreement had expired. All this without prejudice to the

eventual authorization of the parties or, as the case may be, that said information

sara to be considered public domain.

THIRTY-EIGHTH: On October 22, 2020, the METD publishes this note

press:

“The main telephone operators undertake not to affect the con-

sum of data from the RadarCOVID app to its users. (…)

The Secretary of State for Digitization and Artificial Intelligence, C.C.C., has maintained

had a meeting this morning with representatives of the main operators

telephony networks in the country with the aim of establishing ways of collaboration for the

dissemination of the RadarCOVID contact tracing mobile application. The meeting is

framed within a series of sectoral meetings with different actors, institutions,

tutions and companies to explore possible support models for expansion

and implementation among citizens of this digital tool.”

THIRTY NINTH: The Radar COVID application is registered in the Registry of

treatment activities (RAT) of the MSND, SGSDII, in the following terms:

RESPONSIBLE:

GENERAL SECRETARIAT OF DIGITAL HEALTH, INFORMATION AND INNOVATION

OF THE NATIONAL HEALTH SYSTEM. Paseo del Prado, 18. 20. Madrid 28071.

sgsdii@sanidad.gob.es

DELEGATE OF DATA PROTECTION: Head of the General Inspection of

Ministry services. delegateprotecciondatos@mscbs.es

PURPOSES OF TREATMENT:

The purpose of the treatment is to facilitate the traceability of contacts in relation to the

pandemic caused by COVID-19 through user alerts.

LEGAL BASIS OF THE TREATMENT:

• Essential public interest in the specific field of public health, and for the pro-

protection of the vital interests of those affected and of other natural persons protected

of what is established in Regulation (EU) 2016/679 of the European Parliament and of the

Council, of April 27, 2016.

• Organic Law 3/2018, of December 5, on the Protection of Personal Data and ga-

guarantee of digital rights.

• Law 14/1986, of April 25, General Health

•Organic Law 3/1986, of April 14, on Special Measures in Health Matters

Public.

• Law 33/2011, of October 4, General Public Health.

• Royal Decree 463/2020 of March 14, declaring the state of alarm

for the management of the health crisis situation caused by COVID.19 that

attributes to the Ministry of Health the necessary competence throughout the national territory.

nal.

• Ministerial Order SND/297/2020 of March 27, which entrusts the

Secretary of State for Digitization and Artificial Intelligence, of the Ministry of

Economic Affairs and Digital Transformation, the development of new actions.

INTERESTED CATEGORIES

People who have voluntarily downloaded the mobile application have been

diagnosed as a positive case in COVID and have sent the code provided by

the health services of the CCAAs in the application.

PERSONAL DATA CATEGORIES:

The data handled by the application does not allow the direct identification of the

user or your device or your geolocation.

As part of the COVID-19 contagion alert system, the

following data for users who have tested positive for COVID.19 for

purposes specified below:

o The temporary exposure keys with which the user's device has generated

sent random codes (Bluetooth ephemeral identifiers), to the dis-

positives with which the user has come into contact, up to a maximum of 14

past days.

o A 12-digit single-use confirmation code provided by the authorities.

health measures in case of a positive test for COVID.19.

Voluntary questionnaire to collect information on user experience

of the application, understanding of it or perception of privacy, among

others.

RECIPIENTS CATEGORIES:

Application user.

INTERNATIONAL TRANSFERS:

Not foreseen, except legal obligation.

DELETION PERIOD:

Temporary exposure keys and ephemeral Bluetooth identifiers are

stored on the device for a period of 14 days, after which

they are eliminated.

Likewise, the temporary exhibition codes that have been communicated to the service

dor by USERS diagnosed as positive for COVID-19 also se-

They will be removed from the server after 14 days.

TECHNICAL AND ORGANIZATIONAL SECURITY MEASURES:

The security measures implemented correspond to those provided for in the

Annex II (Security measures) of Royal Decree 3/2010, of January 8, by which

the National Security Scheme is regulated in the field of Administration

Electronic and that are described in the documents that make up the Po-

data protection and information security policy of the Ministry.

FORTIETH: In the Evidence Referral Official Letter from the DGSP of the MSND,

registered on October 29, 2021 in the AEPD, it is stated that "As indicated-

ba in the pleadings brief dated June 11, 2021, SEDIA acted as

responsible for processing the information collected by RADAR COVID-19 until

the formalization, on October 13, 2020, of the Agreement between the Ministries

Economics and Digital Transformation and Health. Since then, the Ministry of

Health performed, through the SGSDII, the role of data controller

information. In no resolution, agreement or legal act is the DGSP indicated

as responsible for the treatment of the information generated by the RA-

GIVE COVID-19. Consequently, the DGSP does not hold most of the

required information".

FORTY-FIRST: The advice of the delegate of

data protection of the MSND in the actions investigated.

FORTY-SECOND: On September 9, 2020, the

Open publication of the source code of the “Radar COVID” system:

radar-covid-android – RadarCOVID App for Android - 9 Sept 2020 – GitHub -

RadarCOVID/radar-covid-android at 67a4506cc43a20062e87aebd5caa6be2ea0f6482

radar-covid-ios – iOS Application for RadarCOVID – 9 Sept 2020 – GitHub - Radar-

COVID/radar-covid-ios at 118d6239fc42e369db83e0f2555b62d3e72fc1be

radar-covid-backend-dp3t-server – DPT3 Server - 9 Sept 2020 – GitHub - Radar-

COVID/radar-covid-backend-dp3t-server at 2ea39a5e03ad3da1ff4c7f6567be6b778f-

b79c7d

radar-covid-backend-configuration-server - RadarCOVID-9 service configuration

Sept 2020 - GitHub - RadarCOVID/radar-covid-backend-configuration-server at

ad355dfc3af5d270ecb622f3bc41d013fdb1f81c

FORTY-THIRD: In the response to the request dated 26

October 2020, notified to SEDIA, the existence of a vulnerability is confirmed.

which is corrected in the rise corresponding to October 8, for the following

app versions:

1.Android version 1.0.9

2. Apple, version 1.0.8

It is confirmed that as of October 8, a total of 3,059 codes had been declared.

gos at a national level, although it is true that at the date of publication of the source code

(9/Sep), a total of 574 codes had already been reported.

FORTY-FOURTH: In January 2022, the following information continues to be provided:

training in the "Frequently Asked Questions" of the website: https://radarcovid.gob.es/faq-da-

personal-and-privacy:

How is my privacy protected?

Throughout the design and development process of Radar COVID, the protection

of your privacy has been a priority.

Here is a list of some of the measures with which Radar COVID pro-

get your data:

 The application does not collect any data that allows you to trace your identity.

example, it will not ask you and will not be able to know your name, surnames, address

tion, phone number or email address.

By

 The application does not collect any geolocation data, including that of the

GPS. In addition, it does not track your movements either.

cough.

 The Bluetooth Low Energy code that is transmitted to the

through the app is randomly generated and does not contain any in-

training on your smartphone or on you.

 In addition, this code changes several times every hour to protect even

more your privacy.

 The data stored on your mobile phone is encrypted.

 The connections between the application and the server are encrypted.

 All the data, both those that are saved in the device (international codes)

exchanged with other mobile phones) are deleted after 14 days.

 Likewise, the data collected on the server, coming from the telephones

phones where a positive diagnosis for COVID-19 has been reported, are

deleted after 14 days.

 No data stored on mobile phones or on the server allows

the identification neither of the mobile device itself nor of the user thereof

Does Radar COVID share or sell my data?

Radar COVID does not collect personal data of any kind. only store in

mobile devices information about the codes coming from other te-

mobile phones that have been in close proximity to your phone. these codes

they do not allow to identify neither the device nor its user.

The server with which the applications communicate in case of reporting a

positive diagnosis by COVID-19, it only stores the codes that it has generated

The infected person's phone has been hacked in the last 14 days. Again, it's-

These codes are random and do not allow to identify neither the mobile device nor the

Username.

For all of the above, Radar COVID does not handle information that may be

sold or used for any commercial purpose, including the creation of

profiles for advertising purposes. This project is not for profit.

being created exclusively to help fight the epidemic. I don't know

chart the analysis of aggregated data on the volume of downloads of the application

tion, volume of infected users, or other anonymous indicators and aggregation

gados, for scientific research projects.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each authority of

control and according to what is established in articles 47, 48, 64.2 and 68.1 of the LOPDGDD, the

Director of the AEPD is competent to initiate and resolve this procedure.

II

Article 63.2 of the LOPDGDD determines that: "The procedures processed by the

Spanish Data Protection Agency shall be governed by the provisions of the Regulations

to (EU) 2016/679, in this organic law, by the regulatory provisions

dictated in its development and, as long as they do not contradict them, on a subsidiary basis, by

the general rules on administrative procedures."

III

The DGSP is accused of committing various infractions for violation of articles

The: 5.1.a), 5.2, 12, 13, 25, 28.1, 28.3 and 35 of the RGPD.

The infractions are typified in articles 83.5.a), 83.5.b) and 83.4.a) of the RGPD and

are qualified, for the sole purpose of determining the statute of limitations, in the articles

Articles 72.1.a) and h) and 73.d), k), p) and t) of the LOPDGDD.

Article 83.5.a) and b) of the RGPD indicates:

"Infractions of the following provisions will be sanctioned, in accordance

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

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

of the total global annual turnover of the previous financial year, optionally

dosed for the highest amount:

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

consent under articles 5, 6, 7 and 9;

b) the rights of the interested parties according to articles 12 to 22;

In this regard, the LOPDGDD, in its article 71 establishes that "they constitute infractions

nes the acts and behaviors referred to in sections 4, 5 and 6 of article 83

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

organic".

For the purposes of the limitation period, article 72 of the LOPDGDD indicates:

"Article 72. Infractions considered very serious.

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

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

put a substantial violation of the articles mentioned in that and, in

particularly the following:

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

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

(…)

h) The omission of the duty to inform the affected party about the treatment of their

personal data in accordance with the provisions of articles 13 and 14 of the Regulations

to (EU) 2016/679 and 12 of this organic law."

For its part, article 83.4.a) of the RGPD indicates:

"4. Violations of the following provisions will be sanctioned, in accordance

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

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

of the total global annual turnover of the previous financial year, optionally

being for the highest amount: a) the obligations of the person in charge and of the person in charge

according to articles 8, 11, 25 to 39, 42 and 43;"

For the purposes of the limitation period, article 73 of the LOPDGDD indicates:

"Article 73. Infringements considered serious. Depending on what is established by the

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 result

appropriate to effectively apply the principles of data protection.

from the design, as well as the non-integration of the necessary guarantees in the

treatment, in the terms required by article 25 of the Regulation (EU)

2016/679.

(…)

k) Entrust the processing of data to a third party without the prior formalization of a

contract or other written legal act with the content required by article 28.3

of Regulation (EU) 2016/679

(…)

p) The processing of personal data without carrying out a prior assessment of

the elements mentioned in article 28 of this organic law.

(…)

t) The processing of personal data without having carried out the evaluation of the

Impact of processing operations on the protection of personal data

in the cases in which it is required."

Likewise, article 83.7 of the RGPD says:

Without prejudice to the corrective powers of the control authorities under

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

whether, and to what extent, administrative fines can be imposed on authorities

and public bodies established in that Member State.

In this sense, the LOPDGDD in its article 77, under the heading "Regime applicable to

certain categories of data controllers or processors", establishes the

Next:

"1. The regime established in this article will be applicable to treatments

of which they are responsible or entrusted:

(…)

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

autonomous units and the entities that make up the Local Administration.

(…)

2. When the persons in charge or persons in charge listed in section 1

had any of the infractions referred to in articles 72 to 74 of

this organic law, the data protection authority that is competent

will issue a resolution sanctioning them with a warning. The resolution

It will also establish the measures that should be adopted so that the con-
conduct or correct the effects of the infraction that had been committed.
The resolution will be notified to the person in charge or in charge of the treatment, to the
on which it reports hierarchically, where appropriate, and to those affected who have the
Interested party status, if any.
3. Without prejudice to the provisions of the preceding section, the protection authority
data collection will also propose the initiation of disciplinary actions when
there are sufficient indications for it. In this case, the procedure and
The sanctions to be applied will be those established in the legislation on the disciplinary regime.
plinary or sanctioning that results from application. Likewise, when the infractions
are attributable to authorities and directors, and the existence of in-
technical forms or recommendations for treatment that would not have been
duly attended to, the resolution in which the sanction is imposed will include
A reprimand will be issued with the name of the responsible position and the
publication in the corresponding Official State or Autonomous Gazette.
4. The resolutions must be communicated to the data protection authority
that fall in relation to the measures and actions referred to in the
previous sections.
5. They will be communicated to the Ombudsman or, where appropriate, to the analogous institutions
logs of the autonomous communities the actions carried out and the resolutions
tions issued under this article.
6. When the competent authority is the Spanish Agency for the Protection of
Data, it will publish on its website with due separation the resolutions
tions referring to the entities of section 1 of this article, with express indication
identification of the person responsible or in charge of the treatment that would have co-
committed the infraction. When the competence corresponds to a self-governing authority

nomic of data protection will be, in terms of the advertising of these re-

solutions, to the provisions of its specific regulations".

In summary, the LOPDGDD does not authorize the imposition of administrative fines, but rather a sanction

warning, that is, without any economic effect.

IV

Radar COVID is an application for mobile devices that promotes public health.

Public through a COVID-19 infection alert system.

The Execution Decision (EU) 2020/1023 of the Commission of July 15, 2020, which

modifies the Execution Decision (EU) 2019/1765, regarding the exchange

cross-border data transfer between national mobile conflict-tracing applications

tacts and warning to combat the COVID-19 pandemic, defined in article 1

the following concepts:

h) "contact tracing" or "contact tracing": the measures applied to se-

keep track of people who have been exposed to a source of threat

cross-border risk to health, within the meaning of Article 3, letter c) of the Decision

No. 1082/2013/EU of the European Parliament and of the Council (*);

i) "national mobile application for contact tracing and warning": an application integrated

nationally approved software that works on smart devices, particularly

cular smartphones, is typically designed for a specific interaction.

and wide-ranging with web resources and processes proximity data and other informa-

contextual information picked up by many of the sensors found in devices.

smart devices, in order to trace contacts with people infected by the

SARS-CoV-2 and to warn people who may have been exposed to the

SARS-CoV-2; These mobile applications can detect the presence of other devices.

devices that use Bluetooth and exchange information with end servers (back-

end) over the internet;

k) “key”: the unique ephemeral identifier related to a user of the application

reporting that they are infected with SARS-CoV-2, or that they may have been

exposed to SARS-CoV-2;

Likewise, article 4 of the RGPD includes the following definitions:

1) “personal data”: all information about a ***CLAIMAN.3identifi-

each or identifiable ("the interested party"); shall be considered ***CLAIMAN.3identi-

any person whose identity can be determined, directly or indirectly,

mind, in particular by means of an identifier, such as a name,

an identification number, location data, an online identifier or

one or several elements of the physical, physiological, genetic, psychological identity

cultural, economic, cultural or social life of said person;

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

about personal data or sets of personal data, either by procedures

automated or not, such as the collection, registration, organization, structure-

tion, 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”.

5) "pseudonymization": the processing of personal data in such a way that it

cannot be attributed to a data subject without using additional information, provided

that such additional information is listed separately and is subject to measures

technical and organizational measures designed to ensure that personal data is not

are attributed to a natural person ***CLAIMAN.3 identified or identified

ble;

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

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

healthcare, which reveal information about their health status;

Thus, considering the definitions set forth, it has been found that the application

Radar COVID cation, put into operation in different phases, has carried out treat-

tions of the personal data of the users.

This is the result of the proven facts, after being confirmed in the practice of the evidence, that

By the end of the pilot, more than 58,000 total downloads had been achieved, in

specifically 58,652 as indicated in the document "Monitoring 07.24.2020".

As recognized by SEDIA: "Although at first the

possibility of controlling access to the download of the application exclusively to the public

target audience of the pilot, residents, workers or visitors of San Sebastián de la

Gomera, it was finally decided to leave it open due to 3 key factors:

• Complexity of implementation.

• Negative impact on usability by citizens by having to in-

Enter access codes for the download.

• Incorporate a factor unrelated to the application's own operation in the sub-

national deployment post.”

Likewise, it has been confirmed that aggregated information was collected from users of

the application, both from the people who downloaded it, and from the people who assumed the role of positive cases or received alert notifications of risk of contagion.

According to the population figures resulting from the revision of the municipal registers referred to January 1, 2020, with effect from December 31, 2020, published given in Royal Decree 1147/2020, of December 15, which declares official the population figures resulting from the revision of the Municipal Register referring to the 1st of January 2020, the island of La Gomera, had a population of 21,678 residents. in con- Creto, San Sebastián de La Gomera, municipality where the pilot project is being developed, it had a population of 7,779 inhabitants according to the data registered in the INE. It is- cir, the number of total downloads of the application during the pilot project exceeded the number of 58,000 downloads, far exceeding the number of registered residents on the island, which means that the application was downloaded by a very large number of users. higher than initially planned, located in different parts of the national geography. nal.

Regarding the concept of personal data, we must make a couple of clarifications.

In the first place, the concept of "information" provided for in article 4 of the RGPD must understood extensively, as established by the STJUE of December 20, 2017, in case C-434/16, Peter Nowak and Data Protection Commissioner, “evidences the objective of the Union legislator to attribute to this concept a very broad meaning. plio, which is not limited to confidential data or related to privacy, but that can encompass all kinds of information, both objective and subjective, in the form of number of opinions or assessments, provided that they are “about” the person in question”.

Second, that a vast concept of personal data is widely established. identity, which includes the identification of a natural person ***CLAIMAN.3 in a direct or indirect. In this sense, the STJUE of October 19, 2016, in the matter

C-582/14, Patrick Breyer and Bundesrepublik Deutschland, clearly states that

“The use by the Union legislator of the term “indirectly” shows that, for

qualify personal data information, it is not necessary that such information per-

mita, by itself, identify the interested party”.

At the national level, we will cite for all the Judgment of the National High Court

(SAN) of March 8, 2002 in which it is indicated that "for there to be a data of ca-

personal nature (as opposed to dissociated data) it is not essential to have a full

coincidence between the data and a specific person, but it is enough that such

identification can be made without disproportionate effort” and “to determine whether

a person is identifiable, we must consider the set of means that can

give to be reasonably used by the person in charge of the treatment or by any

another person, to identify that person.

Recital 26 of the RGPD prevents a series of criteria to decree if a person

physical person ***CLAIMAN.3 is or is not identifiable: “To determine whether a person

physical ***CLAIMAN.3 is identifiable, all means must be taken into account,

such as singularization, which can reasonably be used by the data controller.

or any other person to directly or indirectly identify the person

physical. To determine whether there is a reasonable probability that media will be used

In order to identify a natural person, all objective factors must be taken into account.

assets, such as the costs and time required for identification, taking into account

both the technology available at the time of treatment and technological advances

logical”.

It should be noted that in the first impact assessment provided by SEDIA, fe-

Dated in September 2020, it is determined what data is “generated or to which

that the application accesses”, among which personal data is collected.

A first category is identified with the concept of "Personal Data" provided for in

article 4.1 of the RGPD, within which we include proximity data, or the di-

IP address, which the device uses to connect to the Internet.

Proximity data are data by which a subject is located and are,

per se, personal data. This is made clear in the Guidelines of the European Committee

Data Protection Protocol (CEPD) 04/2020 on the use of location data and

contact tracing tools in the context of the COVID-19 pandemic.

The IP address is also a personal data. This question is found

fully resolved, citing to that effect, and, by all, reports 327/2003 or 213/2004

of the Legal Office of the AEPD in which it is concluded that "although it is not always

possible for all Internet agents to identify a user based on data transferred

ted on the Internet, from this Data Protection Agency we start from the idea of

that the possibility of identifying an Internet user exists in many cases and, therefore,

Therefore, both fixed and dynamic IP addresses, regardless of the type of

access, they are considered personal data resulting from the application of the regulations

It's about data protection.

The jurisprudence of the Supreme Court has also been extensive in recognizing

the IP as personal data and not only in the contentious-administrative jurisdiction.

tive, for all, STS 16/2014, of January 30 (rec. 824/2013).

We cannot fail to cite the Judgment of the Contentious-Administrative Chamber of

the National Court of September 1, 2011 (rec. 625/2009) in which it was

establishes that the IP address is a personal data, understanding that "The criterion of identifiability is basic to understand that the IP address should be considered given as personal data and, therefore, is subject to the same guarantees that result from what is foreseen for any kind of personal data in relation to your treatment […] Applying these criteria, it turns out that we must conclude that what recurring trend in relation to the IP addresses of users of P2P networks clearly enters into the concept of data processing and will therefore force the application of the criteria and general requirements of the concept of data treatment cough."

This prescription is also contained in the STJUE of October 19, 2016, in the Case C-582/14), Patrick Breyer and Bundesrepublik Deutschland, asserting that the IP is personal data for the service provider: “article 2, law tra a), of Directive 95/46 must be interpreted in the sense that an IP address dynamics recorded by an online media service provider on the occasion of the consultation by a person of an Internet site that that provider makes accessible to the public constitutes with respect to said provider a personal data, in the sense of the provision, when he has legal means that allow him to identify to the person concerned thanks to the additional information available to the provider Internet access of said person.

Not forgetting that the Article 29 Group, today replaced by the European Committee on Data Protection, in Opinion 4/2007 on the concept of personal data, considers the following: “The Working Group considers IP addresses as data

about an identifiable person. In this sense, it has declared that "the suppliers of
Internet access and local network administrators can identify by means
reasonable to the Internet users to whom they have assigned IP addresses, since they
systematically record date, time, duration and IP address in a file
dynamic assigned to the Internet user. The same can be said for providers.
of Internet services that maintain a log file on the HTTP server. in is-
In all cases, there is no doubt that we can speak of personal data in the
meaning of Article 2(a) of the Directive.
We must bring up recital 26 of the RGPD that informs: "The principles of
data protection must apply to all information relating to a natural person
***CLAIMANT.3 identified or identifiable. Pseudonymous personal data
which could be attributed to a natural person ***CLAIMAN.3 through the use
the provision of additional information, they must be considered information about a natural person.
ca ***CLAIMAN.3 identifiable. To determine if a natural person ***CLAIM-
MANTE.3 is identifiable, all means must be taken into account, such as the singula-
authorization, which may reasonably be used by the data controller or any
another person to directly or indirectly identify the natural person. To determine
determine whether there is a reasonable probability that means will be used to identify
a natural person, all objective factors must be taken into account, such as
costs and time required for identification, taking into account both the technology
ology available at the time of treatment as technological advances. (…)"
These applications store and process data that, although subjected to procedures
encryption and safeguard measures, remain tied to specific individuals.

In fact, maintaining that users are not identifiable, when the purpose of the transaction

treatment is precisely to identify them, it would be a flagrant contradiction.

This is the result of the proven facts after being confirmed in the practice of the evidence (doc.

14) in the information recognized by SEDIA, through the Results Summary

of the pilot of the Radar COVID contagion alert App, dated 07/27/2020:

-

-

The app is faster than us (contacts are registered and po-

sites updating every day proactively)

The app has more memory than us (it records any close contacts,

even those that may go unnoticed by us)

So, there was data processing and although the referred data did not allow the

direct identification of the user or their device, they did allow their identification

hint.

A second category of personal data, we identify it with the "Data related to the

health" provided for in article 4.15 of the RGPD. Such is the case of the confirmation code

12-digit one-time use provided by health authorities in case of testing

positive for COVID, or the data through which the user is previously warned of

a risk contact, as well as the day the user developed symptoms compatible with

ble with COVID-19.

In these cases, we are dealing with a special category of personal data

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

vo that any of the circumstances provided for in section 2 concur. Therefore, in-

embodies an innate danger and must be subjected to a higher standard of protection.

do.

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

that: "Special protection deserves personal data that, by their nature, are

particularly sensitive in relation to fundamental rights and freedoms,

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

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

two, unless their treatment is allowed in specific situations contemplated

in this Regulation, taking into account that Member States may establish

establish specific provisions on data protection in order to adapt the

application of the rules of this Regulation to the fulfillment of an obligation

legal or to fulfill a mission carried out in the public interest or in the exercise of

public powers conferred on the data controller. In addition to the requirements

specific to that processing, the general principles and other rules should apply.

more of this Regulation, especially with regard to the conditions of license

treatment city. Exceptions to the prohibition must be explicitly established.

general treatment of these special categories of personal data, among

other things when the interested party gives his explicit consent or when it is necessary

specific conditions, in particular when the treatment is carried out within the framework of

legitimate activities by certain associations or foundations whose objective is

allow the exercise of fundamental freedoms.

Determined, therefore, the existence of data processing is a priority

determine the role played by the MINISTRY OF HEALTH -through its

governing bodies-, regarding the Radar COVID application, which has entailed the treatment

processing of personal data, including special categories of personal data

(data related to health).

For this, we will examine the concepts of responsible and in charge of the treatment,

the effects of elucidating, if the then GENERAL DIRECTORATE OF PUBLIC HEALTH,

QUALITY AND INNOVATION -now, GENERAL DIRECTORATE OF PUBLIC HEALTH-, has

adequate their performance to the position that according to the RGPD corresponded to them.

v

We will continue the legal foundation determining and differentiating the concepts

responsible and in charge of the treatment.

Regarding the concept of "Responsible for the treatment", article 4.7 of the RGPD,

He says:

7) “responsible for the treatment” or “responsible”: the natural person ***CLAIM-

MANTE.3 or legal entity, public authority, service or other body that, alone or

together with others, determine the purposes and means of the treatment; if the right of

the Union or the Member States determines the purposes and means of the treatment.

treatment, the data controller or the specific criteria for their appointment.

Underwriting may be established by the Law of the Union or of the Member States.

bros”.

The concept of "Data Processor" provided for in article 4.8 says:

8) “in charge of the treatment” or “in charge”: the natural person ***CLAIM-

MANTE.3 or legal, public authority, service or other body that treats data

personal cough on behalf of the data controller.

The concepts of responsible and in charge of treatment are not formal, but func-

tional and must attend to the specific case.

Therefore, we must focus on the sphere of direction, control or management that the res-

responsible can exercise on the processing of personal data that

act in its power by virtue of that cause and that it would be entirely prohibited to the

charged with the treatment, as expressed in Report 287/2006 of the Cabinet

Legal of the AEPD, of June 20, 2006.

The person in charge of the treatment is from the moment he decides the purposes and the means.

god of treatment, not losing such a condition by leaving a certain margin of

action to the person in charge of the treatment.

This is unquestionably expressed in CEPD Guidelines 07/2020 on the con-

cepts of responsible for the treatment and in charge in the RGPD -the translation is

ours-, “A person responsible for the treatment is the one who determines the purposes and

god of treatment, that is, the why and how of treatment. The person in charge of

treatment must decide on both purposes and means. However, some

more practical aspects of the implementation ("non-essential means") can be left

in the hands of the treatment manager. It is not necessary for the controller to have

really access to the data that is being processed to qualify as responsible

ble”.

The RGPD explicitly introduces the principle of responsibility (article 5.2 RGPD),

that is, the data controller will be responsible for compliance with the provisions

set out in section 1 of article 5 and must be able to prove it “responsibility

proactive dad”.

In this sense, article 5 of the RGPD under the heading “Principles related to the treatment

lie" provides:

"1. The personal data will be:

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

("legality, loyalty and transparency");

b) collected for specific, explicit and legitimate purposes, and will not be processed

subsequently in a manner incompatible with those purposes; according to the ar-

Article 89, paragraph 1, the further processing of personal data for purposes

archive in the public interest, scientific and historical research purposes or

statistics shall not be considered incompatible with the initial purposes ("limitation

of the purpose»);

c) adequate, relevant and limited to what is necessary in relation to the purposes

for which they are processed ("data minimization");

d) accurate and, if necessary, updated; all measures will be taken

reasonable for the personal data to be erased or rectified without delay

that are inaccurate with respect to the purposes for which they are processed ("exactly

your D");

e) maintained in a way that allows the identification of the interested parties during

no longer than is necessary for the purposes of data processing

personal; Personal data may be kept for longer periods

long as long as they are treated exclusively for archival purposes in the interest

public, scientific or historical research purposes or statistical purposes, in accordance

accordance with article 89, paragraph 1, without prejudice to the application of the measures

appropriate technical and organizational measures imposed by this Regulation

in order to protect the rights and freedoms of the interested party ("limitation of the term

of conservation”);

f) treated in such a way as to guarantee adequate security of the damages

personal cough,

including protection against unauthorized or unlawful processing and against

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

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

2. The data controller will be responsible for compliance with the provisions

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

Likewise, article 24 of the RGPD under the heading “Responsibility of the person in charge

of the treatment” provides:

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

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

rights and freedoms of natural persons, the data controller applied

Appropriate technical and organizational measures will be taken in order to guarantee and be able to

show that the processing is in accordance with this Regulation. sayings

measures will be reviewed and updated as necessary.

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

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

part of the data controller, of the appropriate protection policies

of data. (…)”

Determining who decides the means and purposes of data processing is crucial to

establish who is responsible for compliance with data protection regulations

personal data, and in particular who should provide information to people who
download the application about the processing of their personal data, which ones are going to
be your rights, who will be responsible in case of breach of the security of
personal data, etc

Well then, fixed the concepts of responsible and in charge of the treatment, as well
as the obligations of the former derived from proactive responsibility (article
5.2 GDPR), we must highlight the peculiar situation of Public Administrations,
where the person in charge of the treatment is that administrative body that has attributions
given the competences by a legal norm, for the exercise of which it is necessary to carry out
processing of personal data. If there is no competence to carry out
undertake a certain activity, nor does one have to carry out the treatments
that would derive from it. The competition will determine, therefore, the legitimacy
to carry out the treatment. And all of this, based on the premise that, compared to what
happens in the private sphere, in which you can do everything that is not prohibited,
Public Administrations can only undertake what the legal system
allows them, with full submission to the Law and the Right (articles 9.1 and 103.1 of the
Spanish constitution).

This is provided for in article 8 of Law 40/2015, of October 1, on the Legal Regime
of the Public Sector (hereinafter, LRJSP), when it is provided that “the competence
authority is inalienable and will be exercised by the administrative bodies that have it attribution.
as its own, except in cases of delegation or avocation, when they are made in
the terms provided in this or other laws.

The second section of article 8.1 of the LRJSP adds that “The delegation of com-
competitions, management assignments, delegation of signature and substitution do not
alteration of the ownership of the competition, although they do of the determined elements
before its exercise that are foreseen in each case”, in such a way that they establish

mechanisms to assign, where appropriate, the exercise of powers to other bodies.

administrative us.

Specifically, regarding the delegation of powers regulated in article 9 of the

LRJSP, must be published in the official bulletins or newspapers, ensuring the security

that must be guaranteed to citizens, who must know, at all times,

who is the administrative body holding a competence and who is exercising it

acting on behalf of the delegating body.

Within the framework of a delegation of powers, the administrative body in which

residence the ownership of this does not lose its status as data controller

for delegating its exercise to another administrative body. And not only because the resolutions

Administrative regulations adopted by delegation will expressly indicate this circumstance.

circumstance and will be considered issued by the delegating body, but because it maintains

control over data processing, since you can revoke the delegation at any time.

any time or raise a matter when there are circumstances that make it con-

coming.

The competent body, which holds ownership, decides that another exercise the competence.

(including in such an exercise a certain margin of maneuver for the delegated body in the

data processing) without losing control. The delegating body, which is responsible

of treatment, when it provides for another body to exercise the powers, it is re-

deciding on the purposes and means of the treatment.

Similarly, if a management entrustment occurs under the terms of article

11 of the LRJSP does not imply transfer of the ownership of the competition nor of the substantive elements of your exercise.

Holding the competence of an administrative body is a capital issue, because its absence can be determinant of nullity of full right or annulment.

Let us now look at the scope of competence in relation to the treatment carried out to determine who is responsible for the treatment. At first, it seems that they are the national health authorities.

Taking into account the sensitivity of the personal data and the purpose of the treatment of the data, the Commission considers that the applications should be designed in in such a way that the national health authorities (or the entities that carry out a mission carried out in favor of the public interest in the field of health) are data controllers (Section 3.1 of the Communication from the European Commission ropea 2020/C 124 I/01).

This will also contribute to strengthening the trust of citizens and, therefore, the acceptance of the applications (and of the underlying information systems on chains of transmission of infections), in addition to guaranteeing that they comply with the intended purpose of protecting public health.

Thus, the Spanish legislator has provided itself with the necessary and timely legal measures to deal with situations of health risk, such as Organic Law 3/1986, of 14 of April, of Special Measures in the Matter of Public Health (modified by Royal Decree-Law 6/2020, of March 10, adopting certain measures urgent calls in the economic sphere and for the protection of public health, published in the Official State Gazette of March 11, 2020) or Law 33/2011, of March 4, October, General Public Health.

Article 3 of Organic Law 3/1986 states that:

“In order to control communicable diseases, the health authority,

In addition to carrying out general preventive actions, it may adopt the measures

appropriate measures for the control of the sick, of the people who are or

have been in contact with them and the immediate environment, as well

such as those considered necessary in case of risk of a transmitted nature.

sible."

In the same way, articles 5 and 84 of Law 33/2011, of October 4, General of

Public Health refer to the previous Organic Law 3/1986, and to the possibility of adopting

Take additional measures in case of risk of disease transmission. For the

Therefore, in terms of risk of disease transmission, epidemic, health crisis,

etc., the applicable regulations have granted "the health authorities of the different

tas Public Administrations" (article 1 Organic Law 3/1986, of April 14) the

powers to adopt the necessary measures provided for in said laws when

so required by health reasons of urgency or necessity. Consequently, from a

point of view of processing personal data, the safeguarding of essential interests

in the field of public health corresponds to the different health authorities

authorities of the different public administrations, who may adopt the measures

necessary to safeguard such essential public interests in situations of

public health health emergency (Report of the Legal Office of the AEPD

0017/2020).

In case there is any doubt regarding the competences attributed to the MSND, through

Royal Decree 463/2020, of March 14, declaring the state of alarm

for the management of the health crisis situation caused by COVID-19, in the

Article 4.2.d) designates the Minister of Health as the competent authority delegated in

your area of responsibility.

At the same time, as established in article 17.1 of Royal Decree 2/2020, of 12

of January, by which the ministerial departments are restructured, corresponds to the

Ministry of Health "the proposal and execution of the Government's policy on

health, planning and health care, as well as the exercise of the powers

ences of the General Administration of the State to ensure citizens the right

cho to health protection."

To the above, we must add the provisions of Royal Decree 454/2020, of March 10,

zo, which develops the basic organic structure of the Ministry of Health, and

Modifies Royal Decree 139/2020, of January 28, which establishes the

basic organic structure of the ministerial departments, in force since 12

March 2020 until August 6, 2020. Therefore, it was the current rule

at the moment in which the actions of the treatment of the

pilot project.

Article 1 provides that "1. It corresponds to the Ministry of Health, the proposal

and implementation of the Government's policy on health, planning and care.

health care, as well as the exercise of the powers of the General Administration

of the State to ensure citizens the right to health protection", indicates

falling below that "2. The powers attributed in this royal decree are

understood in coordination and without prejudice to those that correspond to other rights

ministerial departments.

Putting things this way, the MSND carries out its functions through various bodies.

managers, among whom was the General Directorate of Public Health, Ca-

ity and Innovation. Article 3 of the aforementioned Royal Decree contained its functions,

including those related to public health surveillance or the actions provided for in the

Law 33/2011, of October 4, General Public Health, competence of the administration

state health care, as well as the development of information systems, the

information management and identification of the protected population and access to

clinical and therapeutic information, among others.

Therefore, in accordance with the provisions of current regulations, the competence in

in relation to the actions that included the pilot project Radar COVID corresponding

put the MSND through the General Directorate of Public Health, Quality and Innovation.

tion, being for the purposes of the processing of personal data, the responsible

ble of the treatment.

This is made clear through various actions carried out by the

I win competent.

Thus, in the first place, we must take into consideration the Ministerial Order SND/

297/2020 of March 27, which entrusts the Secretary of State for Di-

digitization and Artificial Intelligence, of the Ministry of Economic Affairs and Transformation.

Digital mation, the development of new actions.

This Ministerial Order determines that the data controller will be the MSND and the

in charge of the treatment and owner of the application will be the SGAD. That is, it is not expected

specifies which administrative body of the MSND is responsible for the treatment, if not

is attributed to the MSND as a whole.

Although such assignment is not made in connection with the Radar COVID application or

with the Radar COVID pilot project, it is done regarding the "Development of solutions
technology and mobile applications for data collection in order to improve
the operational efficiency of health services, as well as the best care and accessibility
ability on the part of citizens related to the powers of the Mi-
Ministry of Health" and "DataCOVID-19: study of mobility applied to the crisis
sanitary".

If the Ministry had the competence to entrust the aforementioned matters in accordance with
me to the aforementioned Ministerial Order, was also competent to have found
recommended the development of the Radar COVID pilot project, since such action entails
clearly falls within the scope of its competences (a technological solution for
improve the operational efficiency of health services, as well as the best care and
accessibility by citizens). However, as we said, regarding
the Radar COVID pilot project was not entrusted by the Ministry through the Or-
Ministerial Decree SND/297/2020 of March 27.

Secondly, and from the test carried out, it is observed how in relation to the pro-
Radar COVID pilot project, the MSND, through the General Directorate of Public Health
ca, Quality and Innovation participated in all the meetings held in relation to the
same as it appears in the proven facts.

In the meeting called pilot closure application RADAR COVID dated July 31
of 2020 even "the following responsibilities are assigned to the Ministry of Health:
Validation Analysis Report of Conclusions. (…) Working Group Ministry of
Health + CCAA + SEDIA (procedures, code management, update protocols)
tion,…".

In fact, the "Condition specifications for the design, development, pilot and evaluation of
a system that allows contact tracing in relation to the pandemic caused
by Covid-19", dated June 10 and 12, 2020, provides in section 1 under the

heading "Background" that,

“In addition, the General Directorate of Public Health, Quality and Innovation,

of the General Secretariat of Health (Ministry of Health) has given the Approval

OK to a pilot test of contact tracing in relation to COVID-19,

entrusting SEDIA with the development of a mobile application for this purpose”.

Without forgetting, thirdly, that on June 9, 2020, the Director

General of Public Health, Quality and Innovation of the Ministry of Health sent a

letter to the Secretary General of Digital Administration (SGAD) informing him of the approval

good of the Ministry for the development of the pilot test of the mobile application for the

tracing of contacts of COVID-19 that was planned to be carried out in the Community

Autonomous Community of the Canary Islands (without prejudice to which the General Director of the

Public Health, Quality and Innovation that the person responsible for processing the data of

this pilot would be the health authority of the community in which it will be carried out).

All of which shows that the MSND, through the General Directorate of

Public Health, Quality and Innovation, was the competent body and therefore the responsible

aware of the treatment in relation to the Radar COVID pilot project, and not SEDIA,

As the DGSP asserted in its allegations to the initiation agreement of June 11,

2020 and which he reiterated when submitting the test.

In the field of Public Administrations, it is not necessary for there to be a resolution

tion, agreement or legal act that attributes the condition of data controller to

an administrative body, since it will suffice with the attribution of competence provided for in the

legal norm that results in each moment of application. Of the competence attribution

cial it is inferred who is responsible for the treatment.

Furthermore, the MSND, through the General Directorate of Public Health,

Quality and Innovation has determined, for the sake of its competencies, the ends and

god of treatment in relation to the Radar COVID pilot project, giving the go-ahead

good to the project in advance (letter dated June 9, 2020), throughout the

development of the project (participating in all the meetings related to it) and after

the same (validating the Conclusion Analysis Report and approving the

pilot test), establishing who should be entrusted with the material development of the project

pilot COVID Radar. In short, it was this Directorate General that decided to use

new technologies, in the form of a mobile application, as a means of supporting the strategy

identification and follow-up of contacts, conditioning the treatment and

“essential means”.

This evidence is revealed not only through the different actions carried out

developed by the MSND during the Radar COVID pilot project (through the Direc-

General Public Health, Quality and Innovation) but also after it, in

relation to the implementation and use of the Radar COVID application; the Ministry if

guided acting actively for the sake of its powers (through the SGSDII).

Thus, on the one hand, on August 19, 2020, the Interterritorial Council of the National System

National Health, signs an "Agreement for the use of the application "Radar COVID", in the phase of

tests, by the Autonomous Communities and Autonomous Cities” that de-

concludes that the MSND, regarding the processing of personal data, is responsible

of the treatment.

It should be noted, as we indicated in the twenty-third proven fact, that in

dated August 5, 2020, the Royal Decree is published in the Official State Gazette

735/2020, of August 4, which develops the basic organic structure of the

MSND.

Thus, the functions of the current DGSP, formerly the General Directorate of Public Health, Cali-

and Innovation, are included in article 3 of Royal Decree 735/2020, among the

which include those related to public health surveillance or the actions contemplated

das in Law 33/2011, of October 4, General Public Health, competence of the

state health administration, among others.

Some of the powers attributed to the former General Directorate of Public Health

ca, Quality and Innovation, specifically "the development of information systems,

information management and identification of the protected population and access to

clinical and therapeutic information", is now attributed to the SGSDII in article 7.1

of Royal Decree 735/2020, of August 4.

It should be noted, as it is representative of what happened, that the SGSDII did not intervene

in the development of the pilot project. The creation of this body occurs in the month

August 2020 following the approval of Royal Decree 735/2020, of August 4,

that additionally reinforces the structure of the MSND, therefore, it did not even exist

when the pilot project started. However, he did later participate in

the implementation and use of the Radar COVID application.

The SGSDII, a newly created governing body, does nothing but give continuity to the pro-

pilot project on the Radar COVID application initiated by another governing body of the

MSND, as was the DGSP. Both, hierarchically integrated into the structure of the

MSND, with competitions that follow one another over time and with the same personality

legal (article 3.4 LRJPS).

Specifically, on October 15, 2020, the "Resolution of

October 13, 2020, of the Undersecretariat, publishing the Agreement between the

Ministry of Economic Affairs and Digital Transformation and the Ministry of Health,

about the application "Radar COVID"", in which it is indicated that they correspond to the

SGSDII a series of functions derived from a delegation of powers carried out

given by the Ministry of Health "in addition to its obligations as Responsible for the

Treatment of personal data". It is also indicated that “correspond to the

General Secretariat of Digital Health, Information and Innovation of the National System of

Health, in its capacity as Responsible for the processing of personal data,

give the necessary instructions to the SGAD in its capacity as data controller

I lie".

In addition, the Radar COVID application is registered in the Activity Registry of

treatment of MSND, SGSDII, in the following terms:

"RESPONSIBLE:

GENERAL SECRETARIAT OF DIGITAL HEALTH, INFORMATION AND INNOVA-

TION OF THE NATIONAL HEALTH SYSTEM. (…)”

Once again, these later actions in which the MSND assumes its competence

Regarding the Radar COVID application (MSND through the SGSDII), they do nothing but

demonstrate that, if the first time the treatment is registered, it is registered in the RAT

of the MSND, where the specific purpose of this treatment is defined (to facilitate the trace-

bility of contacts), the condition of data controller was also held by

already, previously, regarding the COVID Radar pilot project from which the current

application (MSND through the General Directorate of Public Health, Quality and Inno-

vation), since the competences of the MSND have not changed, but only insofar as

to its internal distribution.

On the other hand, Royal Decree 403/2020, of February 25, which develops the basic organizational structure of the Ministry of Economic Affairs and Digital Transformation gital, provides in its article 1 that the METD is in charge of "the policy of telecommunications tions and for digital transformation, in particular promoting the digitization of Public administrations".

Within this framework, SEDIA has, in accordance with article 8, attributed the functions of “promoting the digitization of the public sector and international coordination and cooperation” ministry and with other Public Administrations with respect to said matters, without judgment of the competences attributed to other ministerial departments”.

Applying the foregoing to the case at hand, it corresponded -from the beginning- to the MSND through the General Directorate of Public Health, Quality and Innovation (now, DGSP), exercise the status of data controller for having attributed the com- petition for the processing of personal data object of the application developed and to SEDIA, through the SGAD, the role of data processor.

However, from the proven facts it can be concluded that SEDIA held the status of

responsible for the treatment -every time that according to the definition of article 4.7 of the RGPD determined the purposes and means of the treatments carried out, from the beginning the project in the month of May 2020, until the Resolution of October 13, 2020, of the Undersecretariat, which publishes the Agreement between the Ministry of Economic Affairs and Digital Transformation and the Ministry of Health, about the "Radar COVID" application, where the SGAD is already recognized as being in charge of

treatment, as stated in the thirty-seventh proven fact.

Let us remember that article 9.1 of the LRJSP provides for the delegation of the exercise of competences, a matter different from what it implies to hold the ownership of the competence.

Inc.

Likewise, in the Second Clause, section 3 of the Resolution of October 13, 2020, a recently created governing body, the SGSDII, is attributed the status responsible for the treatment in accordance with what is stated in the thirtieth proven fact seventh.

Likewise, through the press releases published by the METD, it is found that the SEDIA, from the beginning, acted as if it were the data controller.

This is deduced from the proven facts: fifth, eleventh, twenty-second, thirtieth second and thirty-eighth.

Likewise, on June 23, 2020, in the Reference of the Council of Ministers, the Agreement is published by which the declaration of emergency is taken for contracting the design, development, pilot and evaluation services of a system that allows contact tracing in relation to the pandemic caused by CO-VID-19, with a duration of 5 months, for an amount of 330,537.52 euros, VAT included. do.

Likewise, the Resolution of October 13, 2020, of the Undersecretariat, in its section do Sexto recognizes with the following tenor:

“That in application of these principles, since May 2020, the SGAD has been developing, with the knowledge and agreement of the Ministry of Health, an application for the traceability of contacts in relation to the pandemic mine caused by COVID-19 called “Radar COVID.

During the month of July 2020, with the agreement of the General Directorate of Public Health, Quality and Innovation of the Ministry of Health, the SGAD carried out

successfully carried out the pilot project of the same, whose success guarantees the viability of

the proposed solution for close contact tracing”

In addition, in its ninth section it says:

“That, until now, the Ministry of Health has been collaborating with the

SGAD, owner of the “Radar COVID” application, in the functional adjustment processes

end of it from the perspective of public health, coordinating the protocols

epidemiological management of cases detected through the application, and favoring

promoting the progressive incorporation of the autonomous communities and cities into

its use in the testing phase with real data according to the aforementioned Agreement

of August 19, 2020.”

Likewise, both in the Privacy Policy -in its initial version-, and in the Conditions

tions of Use -in its initial and final version-, the SGAD, is identified as the owner of

the COVID Radar app.

Also in the first version of the impact assessment, dated September

2020, both the MSND and the SGAD are recognized as data controllers

as stated in the thirty-fifth proven fact.

In the second version of the impact assessment sent by SEDIA, it is introduced

as responsible to the DGSP, dependent on the MSND and the SGAD is recognized as

in charge of the treatment, as stated in the thirty-fifth proven fact.

Let us also remember that through Royal Decree 463/2020, of March 14, by the

that the state of alarm is declared for the management of the health crisis situation

caused by COVID-19, article 4.2.d) designates the Minister of Health as

delegated competent authority in its area of responsibility.

We also highlight the document "FAQs RADAR COVID", sent by SEDIA,

on July 21, 2020 to the Agency, which includes in point "A.4" the following

question:

“Is the Government in charge of managing Radar COVID? Yes. COVID Radar

is the application of the Government of Spain and has been developed by the Secretariat

of State of Digitization and Artificial Intelligence dependent on the Vice-presidency

Third Office of the Government together with the Ministry of Health.”

Reference to Ministerial Order SND/297/2020 of March 27 is essential,

by which the Secretary of State for Digitization and Ar-Intelligence is entrusted

official, from the Ministry of Economic Affairs and Digital Transformation, the development of

new actions to manage the health crisis caused by COVID-19

(hereinafter, OM) as stated in the third proven fact.

On the one hand, the purpose of the order is not to provide any legal basis for the treatment.

processing of the data, an issue that refers to the provisions of the RGPD.

On the other hand, this rule is cited as applicable legislation in the Privacy Policy of

clearly and in a more circumvented way in the Specifications, by the

SEDIA, as an enabling title for the development of the Radar COVID application. Nope

However, the OM did not cover this application, but only mobility studies.

performed during the state of alarm, as well as other self-diagnosis that

the Government and some autonomous communities put into operation at the beginning

of the pandemic (see the Agreement between SEDIA and Telefónica Digital España, SLU,

for the operation of the ASISTENCIACOVID19 Application in the context of the situation

tion of health crisis caused by COVID-19, published by Resolution of 30

April 2020). This type of applications tried to generalize the geolocation

tion of users, so they are a poor fit with contact tracing. Let's remember that

the Communication of the European Commission 2020/C 124 I/01, discards the need to

geolocation for the purposes of measuring proximity and close contacts (the community

cation between devices over Bluetooth low energy appears to be more accurate and, therefore,

therefore, more appropriate than the use of geolocation data (GNSS/GPS or

mobile device location data)).

If the MSND had wanted to entrust SEDIA with the development of the Ra-

give COVID, he would have shown his will unequivocally. However, this fact

did not occur

In this regard, the file contains a letter dated June 9, 2020, which

signed by the General Director of Public Health, Quality and Innovation addressed to SEDIA,

where the approval of the MSND for its development is communicated, as collected

in the fifth proven fact.

Something similar happens, with the referral to Royal Decree-Law 21/2020, of June 9; neither-

co this normative provision serves as an enabling title for SEDIA to develop

the COVID Radar app.

This is so, because although article 5 provided for the adoption of plans and strategies for

action to deal with health emergencies, through coordinated actions in

public health, taking into account the different levels of risk of exposure and transmission

community awareness of the COVID-19 disease for the development of the different activities

contemplated in the royal decree-law, article 26 referred to a certain content

mined in terms of the "Provision of essential information for the traceability of con-

tacts” addressed to:

“The establishments, means of transport or any other place, center or entity

public or private entity in which the health authorities identify the need

ability to carry out traceability of contacts, they will have the obligation to provide the

health authorities the information they have or that is requested

regarding the identification and contact details of persons potentially

affected.”

To this must be added article 27 of the aforementioned royal decree-law, which under the heading

"Protection of personal data", determined those who had the condition

responsible for the treatment of health data while the pandemic lasted: the

autonomous communities, the cities of Ceuta and Melilla and the Ministry of Health,

within the scope of their respective competences, in accordance with what is indicated in the pro-

bad seventh.

It is worth mentioning article 26.1 of the RGPD that defines what it means by “Co-

data controllers”:

"1. When two or more managers jointly determine the objectives and

treatment means will be considered co-responsible for the treatment. The

co-responsible will determine in a transparent manner and by mutual agreement their responsibilities.

respective responsibilities in the fulfillment of the obligations imposed by

this Regulation, in particular regarding the exercise of the rights of the

interested party and their respective obligations to supply information to which

referred to in articles 13 and 14, except, and to the extent that, their responsibilities

are governed by the law of the Union or of the Member States that are

apply to them. Said agreement may designate a point of contact for

interested. (…)”

In this case, it does not seem that the MSND -through its governing bodies-, and the SE-

DIA, have jointly determined the objectives, the means of treatment or their

respective responsibilities, so the condition of correspondence would be ruled out.

responsible for the treatment.

Recital 79 of the GDPR should be highlighted, which says:

“The protection of the rights and freedoms of the interested parties, as well as the res-

responsibility of those responsible and in charge of the treatment, also in what

regarding the supervision by the control authorities and the measures

adopted by them, require a clear attribution of responsibilities in

under this Regulation, including cases where a controller de-

terminate the purposes and means of processing jointly with other controllers

bles, or in which the treatment is carried out on behalf of a person in charge.”

Also note that the MSND in response to the request dated December 4

of 2020, informs this Agency of the following:

"two. The Ministry of Health exercises the role of data controller through

of the General Secretariat of Digital Health, Innovation and Information of the SNS

(SGSDII), and the General Secretariat of Digital Administration (hereinafter, SGAD),

dependent on the Secretary of State for Digitization and Artificial Intelligence

(hereinafter, SEDIA), of the Ministry of Economic Affairs and Digital Transformation.

gital, performs the role of data processor

.

3. This has been the case since the signing of the Agreement signed between the two ministries between the Mi-

Ministry of Economic Affairs and Digital Transformation and the Ministry of Health

information about the "RADAR COVID" application, published in the BOE of

10/15/2020, (…)”

From the above, several things can be inferred:

One: That SEDIA held the status of data controller, but without co-

legal cover to carry it out. He was responsible for data treatment

referred to in the factual records, since according to the definition of the

Article 4.7 of the RGPD determined the purposes and means of the treatments carried out

(in addition to the appearance before the citizens as responsible for the treatment).

Two: SEDIA was not the competent body to process personal data

in relation to the intended purposes, so that the lack of competence determines

There is no lack of legitimacy in the terms of articles 6 and 9 of the RGPD.

As we have explained previously, the legitimacy to carry out a treatment

In the field of Public Administrations, it is inextricably linked to the

competence of the administrative body that holds it, since only the one that is the

The applicant can decide on the means and purposes of the treatment. Likewise, it is also not

produced prior to the Resolution of October 13, 2020, delegation of

any jurisdiction that would allow the exercise of jurisdiction.

Three: The MSND, through the General Directorate of Public Health, Quality and Innovation

tion, was responsible for processing the data object of the Radar CO-

VINE. However, he did not act as such despite having been assigned the competence -of

inalienable character -, without previously using the Resolution of 13

of October 2020, any of the techniques provided for in articles 9 and following of

the LRJSP, to attribute its exercise to another body (which would be in charge for such purposes

of the treatment).

The facts described are constitutive of the infractions established in articles

83.4.a) and 83.5.a) of the GDPR.

SAW

Let us continue with the legal regime related to those in charge of the treatment that

article 4.8 of the RGPD, already mentioned, thus, recital 81 says:

“To ensure compliance with the provisions of this Regulation

regarding the treatment carried out by the person in charge on behalf of the person in charge.

possible, when entrusting treatment activities to a person in charge, they must resort to

only to processors who offer sufficient guarantees, in particular as regards

in terms of expertise, reliability and resources, for the

application of technical and organizational measures that meet the requirements of the

this Regulation, including the security of the treatment. The adherence of the manager

to an approved code of conduct or approved certification mechanism.

can serve as an element to demonstrate compliance with the obligations

by the person in charge. The treatment by a person in charge must be governed by a

contract or other legal act in accordance with the Law of the Union or of the States

members that links the person in charge with the person in charge, that sets the object and the

treatment, the nature and purposes of the treatment, the type of personal data

stakeholders and categories of stakeholders, taking into account the roles and responsibilities

specific abilities of the person in charge in the context of the treatment that has to be carried out.

carried out and the risk to the rights and freedoms of the interested party. The answer-

saber and keeper may choose to rely on an individual contract or on a

standard contractual clauses to be adopted directly by the Commission or first

adopt a supervisory authority in accordance with the consistency mechanism

and later the Commission. Once the treatment on behalf of the

responsible, the person in charge must, at the choice of the former, return or delete the data.

personal rights, unless the law of the Union or of the Member States applied

cable to the person in charge of the treatment obliges to keep the data."

Secondly, article 28 of the RGPD under the heading "In charge of the treatment-

to" has:

"1. When a treatment is going to be carried out on behalf of a person in charge of the

treatment, this will only choose a person in charge who offers sufficient guarantees

to apply appropriate technical and organizational measures, so that the

treatment is in accordance with the requirements of this Regulation and guarantees

the protection of the rights of the interested party.

2. The person in charge of the treatment will not resort to another person in charge without the authorization

prior written, specific or general, of the person in charge. In the latter case, the

manager will inform the person in charge of any change foreseen in the incorporation

tion or substitution of other managers, thus giving the person in charge the opportunity

to oppose such changes.

3. The treatment by the person in charge will be governed by a contract or other legal act

in accordance with the Law of the Union or of the Member States, which binds the

charged with respect to the person in charge and establish the object, duration, nature

nature and purpose of the treatment, the type of personal data and categories of interest

sados, and the obligations and rights of the person in charge. Said contract or legal act

co shall stipulate, in particular, that the processor:

a) will process personal data only following documented instructions

responsibilities of the controller, including with regard to transfers of personal data

transfers to a third country or an international organization, unless it is obliged to

this under the law of the Union or of the Member States that applies

to the manager; in this case, the person in charge will inform the person in charge of that requirement

prior to treatment, unless such Law prohibits it for important reasons.

tes of public interest;

b) will guarantee that the persons authorized to process personal data have

already committed to respecting confidentiality or are subject to an obligation

confidentiality of a legal nature;

c) take all necessary measures in accordance with article 32;

d) will respect the conditions indicated in sections 2 and 4 to resort to another

treatment manager;

e) will assist the data controller, taking into account the nature of the processing, through

through appropriate technical and organizational measures, whenever possible,

so that it can fulfill its obligation to respond to requests that

have as their object the exercise of the rights of the interested parties established in

chapter III;

f) will help the controller to ensure compliance with the statutory obligations

established in articles 32 to 36, taking into account the nature of the treatment

and the information available to the person in charge;

g) at the choice of the person in charge, will delete or return all personal data

once the provision of treatment services ends, and will delete the co-

existing pias unless the retention of personal data is required

under the law of the Union or of the Member States;

h) will make available to the person in charge all the information necessary to determine

show compliance with the obligations established in this article,

as well as to allow and contribute to the performance of audits, including inspections

tions, by the person in charge or another auditor authorized by said person.

ble.

In relation to the provisions of letter h) of the first paragraph, the manager informs

shall immediately notify the controller if, in his opinion, an instruction violates the

this Regulation or other provisions regarding data protection of

the Union or the Member States.

4. When a person in charge of the treatment resorts to another person in charge to carry out

carry out certain treatment activities on behalf of the person in charge, it is im-

will put this other person in charge, through a contract or other legal act established

under the law of the Union or of the Member States, the same obligations

data protection regulations than those stipulated in the contract or other legal act.

agreement between the person in charge and the person in charge referred to in section 3, in particular

cular the provision of sufficient guarantees for the application of technical and

appropriate organizational arrangements so that the treatment is in accordance with the dis-

positions of this Regulation. If that other person in charge breaches his obligations

data protection regulations, the initial processor will remain fully

responsible to the data controller with regard to compliance

fulfillment of the obligations of the other person in charge.

5. The treatment manager's adherence to a code of conduct approved by

pursuant to article 40 or to a certification mechanism approved pursuant to art.

Article 42 may be used as an element to demonstrate the existence of the ga-

sufficient guarantees referred to in sections 1 and 4 of this article.

6. Without prejudice to the fact that the person in charge and the person in charge of the treatment celebrate a

individual contract, the contract or other legal act referred to in paragraphs

3 and 4 of this article may be based, totally or partially, on the clauses

standard contracts referred to in sections 7 and 8 of this article, including

even when they form part of a certification granted to the person in charge or

loaded in accordance with articles 42 and 43.

7. The Commission may establish standard contractual clauses for the matters to which it is

referred to in sections 3 and 4 of this article, in accordance with the procedure

of examination referred to in article 93, paragraph 2.

8. A supervisory authority may adopt standard contractual clauses for the

matters referred to in sections 3 and 4 of this article, in accordance

with the coherence mechanism referred to in article 63.

9. The contract or other legal act referred to in sections 3 and 4 shall include

in writing, including in electronic format.

10. Without prejudice to the provisions of articles 82, 83 and 84, if a person in charge of the

treatment infringes this Regulation by determining the purposes and means of the

treatment, will be considered responsible for the treatment with respect to said

treatment."

Thirdly, article 29 of the RGPD under the heading “Processing under the authority

of the person in charge or of the person in charge of the treatment” establishes:

“The person in charge of the treatment and any person acting under the authority of the

person in charge or of the person in charge and has access to personal data may only

such data following the instructions of the person in charge, unless they are obliged to

bound to it by virtue of the Law of the Union or of the Member States.”

For its part, article 33 of the LOPDGDD under the heading “Responsible for processing

to” has:

"1. Access by a data processor to personal data

that are necessary for the provision of a service to the person in charge are not

will be considered data communication provided that what is established in the

Regulation (EU) 2016/679, in this organic law and in its implementing regulations.

roll.

2. You will be considered the data controller and not the data processor.

who in his own name and without proof that he acts on behalf of another,

establish relationships with those affected even when there is a contract or legal act

with the content established in article 28.3 of Regulation (EU) 2016/679. Is

provision will not be applicable to treatment orders carried out within the framework

of public sector contracting legislation. It will also have the consideration

tion of responsible for the treatment who, appearing as the person in charge, used the

data for their own purposes.

3. The person in charge of the treatment will determine if, when the provision of

the services of the processor, the personal data must be destroyed, returned

to the person in charge or delivered, where appropriate, to a new person in charge. will not proceed

Destruction of the data when there is a legal provision that requires its con-

preservation, in which case they must be returned to the person in charge, who will guarantee their

conservation while such obligation persists.

4. The person in charge of the treatment may keep, duly blocked, the

data insofar as responsibilities could arise from their relationship with the person responsible.

treatment saber.

5. In the field of the public sector, the powers of the public sector may be attributed.

a data processor to a certain body of the General Administration

of the State, the Administration of the autonomous communities, the Entities

that make up the Local Administration or the Organizations linked to or dependent on

of the same through the adoption of a regulatory norm of said com-

petitions, which must incorporate the content required by article 28.3 of the Re-

regulation (EU) 2016/679."

In this way, taking into account the definitions of responsible and in charge of the

treatment contained both in the RGPD, and in the LOPDGDD, we reiterate must

considered that the defining criterion of the condition of data controller

is given by the power to determine the purposes and means of treatment, as

that the person in charge must limit his action to following the instructions of the person in charge.

responsible, being deemed responsible in the event that it determines ends and means, that is, if

uses for its own purposes the personal data that are within the scope of

tion and control of the person in charge of the treatment in relation to the treatment object of

order, without prejudice to the fact that you may incur an infringement of the RGPD with said action.

tuation.

Consequently, the existence of a data processor will be delimited by

the concurrence of two characteristics derived from the aforementioned regulations. From one side,

the impossibility of deciding on the purpose, content and use of the treatment and,

On the other hand, the non-existence of a direct relationship between the users and the person in charge,

that must in any case act in the name and on behalf of the person in charge as if the re-

relationship was between this one and those.

The essence of the function of data processor is that the personal data

are processed in the name and on behalf of the data controller.

The person in charge of the treatment can only carry out treatments on the instructions

documentation of the controller, unless required to do so by law

of the Union or of a Member State, a circumstance that does not occur in the case analysed.

ted.

In relation to the Radar COVID pilot project, the General Directorate of Public Health

ca, Quality and Innovation, as data controller, had to articulate its relationship

with the person in charge of the treatment through a contract or a similar legal act

to link them. The contract or legal act must be in writing, including in

electronic kill. The possibility of regulating this relationship through a legal act

unilateral data controller is one of the novelties provided for in the

GDPR. In any case, it should be a legal act that establishes and defines

the position of the person in charge of the treatment, as long as that act legally binds

directly to the person in charge of the treatment. This would be the case, for example, of a resolution

administrative solution that was notified to the person in charge of the treatment. In which-

In any case, whether it was an agreement or another legal act, its content had to meet

meet the requirements established in the RGPD.

Thus, in the case analyzed and with respect to the Radar COVID pilot project, let us remember that

There is only one letter from the General Director of Public Health, Quality and In-

novation, dated June 9, 2020, with content that does not meet the requirements

agencies of article 28 of the RGPD, because:

-. The treatment must be regulated by a contract or legal bond that establishes

ca the object, the duration, the nature, the purpose of the treatment, the type of data

data, the categories of interested parties, and the obligations and rights of the res-

responsible.

-. The engagement contract shall specifically stipulate that the person in charge treats

will personal data only by following the documented instructions of the

responsible, so the person in charge of treatment should not enter in the application

cation other processing of personal data that the controller may not know

cer, such as those that can be introduced by including in the application libraries of

third parties for advertising, analytical, or other purposes.

-. The contract of assignment will stipulate that the person in charge of the treatment will take the

measures indicated by the person in charge regarding the security of the treatment, in-

specifically including good development practices and taking into account the

privacy by design and by default from the very conception of the application.

tion.

In the meetings related to the Radar COVID pilot project in which

members of the General Directorate of Public Health, Quality and Innovation, no

He received no instructions from the governing body.

In addition, there is also no Ministerial Order similar to the Ministerial Order SND/

297/2020 of March 27, in which SEDIA is entrusted with the development and implementa-

Mention of the Radar COVID pilot project, which could, at least, formally grant it

mind the category of data processor.

These "instructions" are not enough to articulate the relationship between responsible and

in charge of the treatment, a relationship that cannot be considered as a mere formation

administrative malice or as an exchange of opinions, but as a means to

seek the defense and protection of the Fundamental Right to data protection

of a personal nature, especially when the relationship is established between Administrations

Public authorities to whom it corresponds “to promote the conditions so that freedom and

equality of the individual and of the groups in which he is integrated are real and effective; rowing-

see the obstacles that prevent or hinder its fullness and facilitate the participation of all

citizens in political, economic, cultural and social life”, article 9.2 of the

Spanish constitution.

But it is also that, in addition, the action of the person in charge of the treatment is not exhausted in the

election of the person in charge of the treatment and the corresponding subscription of the contract of

in charge of the treatment, but must be deployed throughout the entire assignment,

as we will show below.

CEPD Guidelines 07/2020 on the concepts of data controller

and commissioned in the RGPD, of September 2, 2020, establish that -the translation

it's ours- “97. The obligation to use only data processors "who

provide sufficient guarantees" contained in article 28, section 1, of the RGPD

it is an obligation

. It does not end at the moment when the person in charge and the

charged with the treatment enter into a contract or other legal act. Instead, the response

sable should, at appropriate intervals, verify the clerk's warranties, including

through audits and inspections when appropriate".

keep going

In the same way that the person responsible for the treatment audits those treatments that

you perform directly and on your own, you must control the treatments that others perform

for your assignment. In particular, it must be ensured that the instructions supplied

requirements are met and that the technical and organizational security measures are carried out

effect, ensuring compliance with the obligations established in articles

32 and following of the RGPD.

From the proven facts, the absence of the continuous control that must be deployed is concluded.

garge the person in charge of the treatment in relation to the action of the person in charge of the treatment

lie with respect to the entrusted order. In the case examined, the action

of the data controller regarding the approval of the Radar pilot project

COVID and to carry out the validation of the Analysis of Conclusions report of the project

pilot, determine the insufficiency of the supplied instructions that were not de-

duly documented (article 28.3.a) of the RGPD).

The facts described are constitutive of the infraction established in article

83.4.a) of the GDPR.

Recital 39 of the GDPR says:

7th

“The principle of transparency requires that all information and communication regarding to the processing of said data is easily accessible and easy to understand, and that use simple and clear language. This principle refers in particular to the information of the interested parties on the identity of the person in charge of the treatment and the purposes of the same and the information added to guarantee a treatment fair and transparent with respect to the natural persons affected and their right to obtain confirmation and communication of personal data concerning them that are subject to treatment.”

In the first version of the application planned for the Pilot Program on the Island of Gomera (July 2020), the information regarding the

Privacy:

Conditions of use: ***URL.6

Privacy Policy: ***URL.7

However, none of them defined who was responsible or in charge of the treatment.

I lie.

In the "Conditions of use", there was only a clause related to the ownership of the application:

5. Owner of the application The General Secretariat of Digital Administration (SGAD), dependent on the Secretary of State for Digitization and Intelligence Artificial of the Ministry of Economic Affairs and Digital Transformation, is the TI-TULAR of the Radar COVID application. (…)

Regarding the accessibility of the Radar COVID application, in the month of September, an action was opened by the Ombudsman against SEDIA for the lack of adaptation of the contagion tracking application, which was not accessible, especially Especially for people with visual problems. The same Secretary of State of

Digitization and Artificial Intelligence recognized this circumstance through the Twitter channel.

tter.

On the other hand, there have been several revisions in the "Terms of use" and

Existing “Privacy Policy”.

Let us not forget that the person in charge must observe the same principles when communicating

nica both initial privacy statements and in any substantive changes

essential or important that you enter later.

The incorporated modifications are considerable and affect various aspects.

On July 28, 2020, SEDIA provides a revised document of "Conditions

of use”, where it is observed that they have eliminated point 5, relative to the “Holder of the application”.

cation”, replacing it with “Intellectual and industrial property”.

It is not clear who is responsible for the treatment nor the data of the delegate.

data protection law, which is not even mentioned in the privacy policy.

Let us refer to CEPD Guidelines 04/2020, which in section 25 say:

“To ensure accountability, it must be clearly defined who is

those responsible for data processing in this type of application. in opinion

of the EDPB, it could be the national health authorities, although it is possible to

see also other formulas. In any case, if the deployment of scraping applications

contact management involves different agents, it is important that their roles and

responsibilities are clearly delineated from the outset and explained

quen users.”

The Privacy Policy in its final version informs:

“This application is responsible for processing both the Ministry of

Health, as well as the Autonomous Communities. Likewise, the General Secretariat

The General Director of Digital Administration acts as the person in charge of the treatment.

At the national level, the person responsible for processing your data as a user of

“COVID Radar” is:

As part of the COVID-19 contagion alert system, data will be processed

the following data for users who have tested positive for COVID-19

for the purposes specified below:

Name: Ministry of Health.

Address: Paseo del Prado 18-20, 28014 Madrid

The General Secretariat of Digital Administration, as the owner of the application

cation and based on the order of the treatment entrusted by the Ministry of

Health, will carry out the following processing operations: (...)”

In relation to the categories of data, the initial version collects information:

“ − The temporary exhibition keys (…)

− A 12-digit one-time confirmation code (…)

− Voluntary questionnaire to collect information on the experience of

use of the application, understanding of it or perception of privacy

among others."

And the final version:

“− The keys of temporary exhibition (…)

− A 12-digit one-time confirmation code (…)

− The user's consent, if applicable, for the remission of exposure keys.

temporary assignment to the European Node for Interoperability of Tracing Applications

contacts.

− The notice of notification of exposure, in order to collect anomalous statistics

minimum and aggregate of the volume of notifications produced by the system through

of contact tracing. These data allow estimating how many users have been

alerted by the Application, of a potential risk of infection, without being able to trace

his identity."

Privacy policies must be concrete and specific about the treatment of

personal data that is carried out.

The same happens with the bases of legality: they are not specified sufficiently

clear in the initial version or in the final version:

Initial version:

“10. What is the legitimacy for the treatment of your data? The data generated

two will be treated legitimately with the following legal bases:

− The user's free, specific, informed and unequivocal consent of the

USER, making this privacy policy available to you, which must-

You will accept by marking the box provided for this purpose.

− Reasons of public interest in the field of public health, such as the protection

against serious cross-border threats to health (article 9.2 i) of the RGPD),

for the treatment of health data (for example, the state of a person

infected or information about symptoms, etc.).

− Fulfillment of a mission carried out in the public interest or in the exercise of

public rights conferred on the data controller (article 6.1 e) RGPD).

− Archive purposes of public interest, scientific or historical research purposes or

statistical purposes (article 9.2 j) RGPD).”

In the definitive version it eliminates question number 10 and refers to the bases in a

generic It also eliminates the base relative to article 9.2.j) and introduces 9.2.h).

“All information will be collected for strictly public interest purposes in the

field of public health, and in view of the decreed health emergency situation,

in order to protect and safeguard an interest essential to people's lives,

in the terms described in this privacy policy, and in accordance with the articles

6.1.a), 9.2.a), 6.1.c), 6.1.d), 6.1.e), 9.2.c), 9.2.h) and 9.2.i).

The applicable legislation is listed below:

~

Regulation (EU) 2016/679, of April 27, 2016, regarding the protection

of natural persons with regard to the processing of personal data

them and the free movement of these data and by which the Directive is repealed

95/46/EC (General Data Protection Regulation).

~

Law 33/2011, of October 4, General Public Health.

Law 14/1986, of April 25, General Health.

~

~

~

~

Royal Decree Law 21/2020, of June 9, on urgent preventive measures

tion, containment and coordination to deal with the occasional health crisis

affected by COVID-19.

~

Agreement of October 9, 2020, between the METD (SEDIA) and the MSND

about the “Radar COVID” app.

Regarding the purposes of the treatment, the initial version informs:

“ − Offer you information on contacts considered to be at risk of exposure to

the COVID-19.

− Provide you with practical advice and recommendations for actions to follow

According to situations of risk in the face of quarantine or self-quarantine-

na.”

And the definitive version adds:

“− The data will always and only be used anonymously for statistical purposes.

ethical and epidemiological. “

Let us remember that it eliminated the basis of article 9.2.j) of the RGPD.

Lastly, regarding the information regarding Who has access to your data?

initial release reports:

“The Owner of the Application may give access or transmit the data to third parties pro-

service providers, with whom it has signed treatment order agreements.

processing of data, and that they only access said information to provide a

service in favor and on behalf of the person in charge.”

And the definitive version adds:

“The data managed by the mobile application (daily keys for temperature exposure)

ephemeral Bluetooth identifiers) are stored only on the device.

user's site for the purposes of being able to make calculations and notify the USER about

your risk of exposure to COVID-19.

Only in the case of reporting a positive diagnosis for COVID-19, the passwords for

temporary exposure of the last 14 days generated on the device, and under the

explicit and unequivocal consent of the USER, are uploaded to the server for

its dissemination to all USERS of this system.

These keys have nothing to do with the identity of the mobile devices.

them or with personal data of the USERS of the Application.

Reported exposure notification advisories are only used for the management of

generation of aggregated and anonymous statistical data.”

In short, the Privacy Policy has been modified in numerous aspects until-

to such an extent that it represents an increase of almost 700 words with respect to the initial version.

cial.

Article 5.1.a) of the RGPD must be connected with the provisions of article 12.1 and 2 of the RGPD that defines the regime applicable to the "Transparency of information, co-communication and modalities of exercising the rights of the interested party":

"1. The person responsible for the treatment will take the appropriate measures to facilitate the interested all information indicated in articles 13 and 14, as well as any communication under articles 15 to 22 and 34 relating to processing, in concise, transparent, intelligible and easily accessible form, with clear language and simple, in particular any information directed specifically at a child. The information will be provided in writing or by other means, including, if applicable, by electronic means. When requested by the interested party, the information may be be verbally requested provided that the identity of the interested party is proven by other media.

2. The data controller shall facilitate the interested party in the exercise of their rights. chos by virtue of articles 15 to 22. (…)"

In the same sense, recital 60 of the RGPD provides that:

"The principles of fair and transparent processing require that the user be informed aware of the existence of the treatment operation and its purposes. The responsible-treatment must provide the interested party with as much complementary information taria is necessary to guarantee a fair and transparent treatment, given account of the specific circumstances and context in which the data is processed. personal cough. The interested party must also be informed of the existence of the profiling and the consequences of such profiling. If you give them-personal data are obtained from data subjects, they must also be informed of if they are obliged to provide them and the consequences in case they do not do so. close".

The initial version of the Privacy Policy denied the exercise of rights 15 to

22 of the GDPR:

“8. What are your rights and how can you control your data? Given that the

Radar COVID application does not store personal data, the

rights of access, rectification, deletion, limitation, opposition and portability,

as well as not to be subject to decisions based solely on the autho-

tomato of your data. In any case, we are obliged to tell you that

attends at all times the right to file a claim with the Agency

Spanish Data Protection Agency (www.aepd.es).”

The definitive Privacy Policy recognizes the aforementioned rights, except that of

portability.

In short, the then GENERAL DIRECTORATE OF PUBLIC HEALTH, QUALITY AND IN-

NOVACIÓN, now, GENERAL DIRECTORATE OF PUBLIC HEALTH, being the responsibility

responsible for the treatment, did not take the appropriate measures to facilitate the interested parties

information in the terms established in articles 12 and 13 of the RGPD.

This information should have been provided in a concise, transparent, intelligible and

easy access, with clear and simple language, and, in addition, where appropriate, viewable.

This is especially pertinent in situations such as the one that occurs, in which the

proliferation of agents and the technological complexity of the application make it

difficult for citizens to know and understand if they are being collected, by whom and with

what purpose, personal data that concerns you, as in the case analyzed.

Even in a situation such as the one that occurred, compliance with the

data protection regulations. The legal system contains provisions applicable

cables to the control of epidemics and their spread, especially in the event of catastrophes

natural or of human origin (considering 46, articles 6.1.e), 6.1.d), 9.2.g) and i) of the

GDPR).

In fact, the declared state of alarm revealed the protagonism and relevance

vance of the right to data protection that reaches a substantial meaning, ma-

xime when the processing of special categories of data is at stake.

Add, in addition, a reference to article 13 of the RGPD that, in relation to the “Information

information that must be provided when the personal data is obtained from the interested party.

do” has:

"1. When personal data relating to him is obtained from an interested party, the res-

responsible for the treatment, at the time these are obtained, will provide

all the information indicated below:

a) the identity and contact details of the person in charge and, where appropriate, of their representative.

sitting;

b) the contact details of the data protection delegate, if applicable;

c) the purposes of the processing for which the personal data is intended and the legal basis

ca of treatment; (...);

e) the recipients or the categories of recipients of the personal data, in

Their case;

f) where appropriate, the intention of the controller to transfer personal data to a third party.

certain country or international organization and the existence or absence of a decision

adequacy of the Commission, or, in the case of transfers indicated in the

articles 46 or 47 or article 49, paragraph 1, second paragraph, reference to the

adequate or appropriate warranties and the means to obtain a copy of these or

to the place where they are made available.

2. In addition to the information mentioned in section 1, the person responsible for the

treatment will provide the interested party, at the time the personal data is obtained,

personal, the following information necessary to guarantee a treatment of data

loyal and transparent cough:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

157/168

a) the period during which the personal data will be kept or, when it is not

possible, the criteria used to determine this period;

b) the existence of the right to request from the data controller access to

the personal data relating to the interested party, and its rectification or deletion, or the

limitation of its treatment, or to oppose the treatment, as well as the right to

data portability;

c) when the treatment is based on article 6, paragraph 1, letter a), or the ar-

Article 9, paragraph 2, letter a), the existence of the right to withdraw consent

at any time, without affecting the legality of the treatment based on the

consent prior to its withdrawal;

d) the right to file a claim with a supervisory authority;

(…)

f) the existence of automated decisions, including profiling, to

referred to in article 22, sections 1 and 4, and, at least in such cases, inform

significant insight into applied logic, as well as the importance and consequences

foreseen consequences of said treatment for the interested party.

3. When the data controller plans further data processing

personal data for a purpose other than that for which they were collected, you will provide

to the interested party, prior to said subsequent treatment, information about that

other purpose and any additional relevant information within the meaning of paragraph 2.

4. The provisions of sections 1, 2 and 3 shall not apply when and in the

to the extent that the interested party already has the information."

For its part, article 11 of the LOPDGDD, under the heading "Transparency and information

tion to the affected" indicates:

"1. When the personal data is obtained from the affected party, the person responsible for the

treatment may comply with the duty of information established in art.

Article 13 of Regulation (EU) 2016/679, providing the affected party with the basic information

to which the following section refers and indicating an electronic address

ca or other means that allows easy and immediate access to the remaining

information.

2. The basic information referred to in the previous section must contain,

at least:

a) The identity of the data controller and his representative, if any.

b) The purpose of the treatment.

c) The possibility of exercising the rights established in articles 15 to 22 of the

Regulation (EU) 2016/679.

If the data obtained from the affected party were to be processed for the preparation of

profiles, the basic information will also include this circumstance. In this

case, the affected party must be informed of their right to oppose the adoption
of automated individual decisions that produce legal effects on him
or significantly affect you in a similar way, when this right of
in accordance with the provisions of article 22 of Regulation (EU) 2016/679.
3. When the personal data had not been obtained from the affected party, the res-
responsible may comply with the duty of information established in article
14 of Regulation (EU) 2016/679, providing the latter with the basic information
indicated in the previous section, indicating an electronic address or other means
that allows easy and immediate access to the rest of the information. In
these assumptions, the basic information will also include: a) The categories of data
cough subject to treatment. b) The sources from which the data came."
Thus, the informative duty linked to the guarantees of the right to protection
of data in the terms of article 13 of the RGPD and 11 of the LOPDGDD, is part
of the guarantees linked to the fundamental right to the protection of personal data.
ter personal, which must necessarily be respected.
Emphasize that initially the information regarding the person in charge, destination
or the rights of articles 15 to 22. Nor in the definitive version has
including information regarding the data protection officer.
The lack of information, the absence of transparency, is in itself a vulnerability
regulation of data protection, which has an immediate and direct impact
ta in the exercise of rights by interested persons. So the lack of
knowledge about the treatment, the person in charge of the treatment, the contact data
of the data protection delegate or the simple possibility of exercising the rights
rights conferred in articles 15 to 22 of the RGPD, prevent or hinder the opportunity to
exercise them.
For these reasons, the facts described are constitutive of the infringement established

in article 83.5 a) and b) of the RGPD.

viii

In an increasingly digital world, adherence to data protection by design and

by default plays a crucial role in promoting privacy and protection.

tion of data in society.

The measures applied were not appropriate to achieve the intended objective.

This Agency registered several claims in which a vulnerability was denounced.

ity in the design of the application.

According to SEDIA, this vulnerability was already known by the development team

of Radar COVID, since it appeared in at least one technical document published in

April 2020 by the DP3T team: Privacy and Security Risk Evaluation of Digital Proxi-

mity Tracing Systems.

However, the development team did not find it necessary to resolve this issue in

the first versions since, to exploit this vulnerability, it was necessary to assume

have a remote scenario where the telecommunications operator was interested in

do in obtaining this clinical information from their clients by studying data traffic

generated by Radar COVID apps.

The application was put into service nationwide on August 19, 2020. The vulnerability

This probability was corrected in the rise corresponding to October 8, 2020, for the following

following versions of the application: Android, version 1.0.9, Apple, version 1.0.8.

Recital 78 of the RGPD says:

“The protection of the rights and freedoms of natural persons with respect to
processing of personal data requires the adoption of technical and organizational measures
appropriate measures in order to ensure compliance with the requirements of the
this Regulation. In order to demonstrate compliance with this
Regulation, the data controller must adopt internal policies and apply
Take measures that comply in particular with the data protection principles described
by design and default. Said measures could consist, among others, of reducing
minimize the processing of personal data, pseudonymize as soon as possible
personal data, give transparency to the functions and data processing
personal, allowing interested parties to supervise the processing of data and to
responsible for the treatment create and improve security elements. To the develop-
develop, design, select, and use applications, services, and products that are
used in the processing of personal data or that process personal data to
fulfill their role, producers of the products, services and
applications to take into account the right to data protection when
develop and design these products, services and applications, and to ensure
ensure, with due regard to the state of the art, that those responsible and
data processors are in a position to fulfill their obligations in
matter of data protection. The principles of data protection from the
design and default must also be considered in the context of the con-
public dealings.”

Likewise, recital 83 of the RGPD says:

“In order to maintain security and prevent the treatment from violating the provisions of
this Regulation, the person in charge or the person in charge must evaluate the risks
inherent to the treatment and apply measures to mitigate them, such as encryption. These
measures must guarantee an adequate level of security, including the confidentiality

ciality, taking into account the state of the art and the cost of its application with

regarding the risks and the nature of the personal data that must be protected.

gerse. When assessing risk in relation to data security, consideration should be given to

take into account the risks arising from the processing of personal data,

such as the accidental or unlawful destruction, loss or alteration of personal data

transmitted, stored or otherwise processed, or the communication or access

unauthorized access to said data, which may in particular cause damage and

physical, material or immaterial damages."

Article 25 of the RGPD under the heading "Data protection by design and by

defect" provides:

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

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

versa 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 determining the means of treatment as at the time

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

pseudonymization, designed to effectively apply the principles of

data protection, such as data minimization, and integrate guarantees

necessary in the treatment, in order to meet the requirements of this Regulation-

mento 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

I keep the personal data that is necessary for each of the purposes

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

data collected, to the extent of its treatment, to its term of conservation

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

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

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

In accordance with the above, the design of the application has not had pre-

effectively lays down the principles applicable to data protection.

In the application of technical and organizational security measures, the person in charge

has not taken into consideration the risks that this treatment represented. While

that the treatment of the IP address was necessary for the operation of the application.

tion, the possibility of associating the IP with the rise of a positive test was not. This tra-

Data processing contradicts what is stated in question 8 of the latest version of the

privacy policy, which emphasizes that "these keys have no relation

with the identity of the mobile devices or with the personal data of the USERS

of the application".

And even being aware of the risk, they did not integrate the necessary guarantees to win.

guarantee the confidentiality of the data and the resilience of the systems.

Consequently, the responsibility of the person responsible for the traffic must be established.

treatment for any treatment 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 the trafficking activities

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

In short, this principle requires a conscious, diligent, committed and proactive attitude.

active by the person in charge against all personal data processing

to carry out.

The facts described are constitutive of the infraction foreseen in article 83.4.a)

of the GDPR.

IX

Recital 89 of the RGPD states:

“(…) Therefore, these general obligations of indiscriminate notification must

eliminated and replaced by effective procedures and mechanisms that focus on

train, instead, in the types of processing operations that, by their nature,

size, scope, context and purposes, probably entail a high risk for the de-

rights and freedoms of natural persons. These types of treatment operations

training may be, in particular, those involving the use of new technologies, or

are of a new class and the data controller has not previously performed

mind an impact assessment related to data protection, or if they are

necessary given the time elapsed since the initial treatment.”

Also recital 90 of the RGPD says:

“In such cases, the person in charge must carry out, before the treatment, a

impact assessment relating to data protection in order to assess the par-

particular severity and likelihood of the high risk, taking into account the nature,

scope, context and purposes of the treatment and the origins of the risk. Said evalua-

impact assessment should include, in particular, the measures, guarantees and mechanisms

provided to mitigate the risk, guarantee the protection of personal data and

demonstrate compliance with this Regulation."

Likewise, recital 91 of the RGPD says:

"The foregoing should apply, in particular, to large-scale treatment operations.
scale that seek to process a considerable amount of personal data at the
regional, national or supranational and that could affect a large number of in-
concerned and likely to involve a high risk, for example, because of their sensitivity
possibility, when, depending on the level of technical knowledge achieved,
has used a new technology on a large scale and other treatment operations
that entail a high risk for the rights and freedoms of the interested parties.
two, in particular when these operations make it more difficult for the interested parties
the exercise of their rights. (…)"

Article 35 of the GDPR states:

"1. When a type of treatment, particularly if it uses newer
technologies, by their nature, scope, context or purposes, entails a high risk
for the rights and freedoms of natural persons, the data controller
will carry out, before the treatment, an evaluation of the impact of the operations
tions of treatment in the protection of personal data. A single evaluation
may undertake a series of similar processing operations involving some
similar risks.

2. The person in charge of the treatment will obtain the advice of the delegate of pro-
data protection, if appointed, when conducting the relative impact assessment
to data protection.

3. The data protection impact assessment referred to
Paragraph 1 will be required in particular in the event of:

a) systematic and exhaustive evaluation of personal aspects of natural persons

cas that is based on automated processing, such as profiling,

and on the basis of which decisions are made that produce legal effects for the

natural persons or that significantly affect them in a similar way;

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

Article 9, paragraph 1, or personal data relating to convictions and in-

penal fractions referred to in article 10, or

c) large-scale systematic observation of a publicly accessible area.

4. The control authority shall establish and publish a list of the types of operations

treatment tions that require an impact assessment relative to the production

data protection in accordance with section 1. The Community supervisory authority

It shall communicate these lists to the Committee referred to in article 68.

5. The control authority may also establish and publish the list of types

of treatment that do not require impact assessments related to the protection

of data. The control authority shall communicate these lists to the Committee.

6. Before adopting the lists referred to in paragraphs 4 and 5, the authority of

competent control will apply the coherence mechanism contemplated in art.

Article 63 if those lists include processing activities that are related

with the offer of goods or services to interested parties or with the observation of the behavior

treatment of these in several Member States, or treatment activities that

may substantially affect the free circulation of personal data in the

Union.

7. The evaluation shall include at least: a) a systematic description of

the planned treatment operations and the purposes of the treatment, including,

where appropriate, the legitimate interest pursued by the data controller;

b) an assessment of the necessity and proportionality of the trading operations

treatment with respect to its purpose; c) an assessment of the risks to the de-

rights and freedoms of the interested parties referred to in section 1, and d) the me-

measures planned to deal with the risks, including guarantees, security measures,

and mechanisms that guarantee the protection of personal data, and to demonstrate

comply with this Regulation, taking into account the rights

and legitimate interests of the interested parties and other affected persons.

8. Compliance with the approved codes of conduct referred to in article

article 40 by the corresponding managers or managers, it will be duly

taken into account when assessing the impact of treatment operations

carried out by said managers or managers, in particular for the purposes of

data protection impact assessment.

9. When appropriate, the person in charge will obtain the opinion of the interested parties or

their representatives in relation to the planned treatment, without prejudice to the pro-

protection of public or commercial interests or the security of operations

of treatment.

10. When the treatment in accordance with article 6, paragraph 1, letters c) or

e), has its legal basis in the Law of the Union or in the Law of the State

member that applies to the data controller, such Law regulates the operation

specific ration of treatment or set of operations in question, and it is already

has carried out an impact assessment related to data protection as

part of an overall impact assessment in the context of decision-making

this legal basis, sections 1 to 7 will not apply except if the States

two members consider it necessary to carry out this evaluation prior to the activities

treatment lives.

11. If necessary, the person in charge will examine whether the treatment is in accordance

with the data protection impact assessment, at least when

there is a change in the risk represented by the treatment operations."

Likewise, section 39 of the CEPD Guidelines 04/2020 says:

"Finally, the EDPB considers that an impact assessment must be carried out

Data Protection Agreement (EIPD) before starting to use an application.

cation of this type because it is considered that the treatment may entail a

high risk (health data, prior large-scale adoption, systematic follow-up)

tico, use of a new technological solution). The CEPD strongly recommends

citedly the publication of the DPIA."

The AEPD, in compliance with the mandate provided for in article 35.4 of the RGPD, published

an indicative and non-exhaustive list of types of treatment that require an evaluation

impact statement regarding data protection. It is based on the established criteria

by the Article 29 Working Group in the guide WP248 "Guidelines on the evaluation

data protection impact statement (EIPD) and to determine whether the processing

"probably entails a high risk" for the purposes of the RGPD", complementing

do the provisions of the Guidelines.

Among the treatments in which an EIPD is necessary, there are:

"3. Treatments involving observation, monitoring, supervision,

geolocation or control of the interested party in a systematic and exhaustive way, including

including the collection of data and metadata through networks, applications or in

public access areas, as well as the processing of unique identifiers

that allow the identification of users of services of the information society

training such as web services, interactive TV, mobile applications,

vile etc

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

referred to in article 9.1 of the RGPD, data related to convictions or infractions

criminal penalties referred to in article 10 of the RGPD or data that allow

determine the financial situation or equity solvency or deduce information

tion on persons related to special categories of data.

(…)

7. Processing involving the use of large-scale data. To determine

If a treatment can be considered on a large scale, the criteria will be considered.

established in guide WP243 “Guidelines on protection delegates”

Data Protection (DPD)” of the Article 29 Working Group.

(…)

10. Treatments that imply the use of new technologies or a use

innovator of established technologies, including the use of technologies

on a new scale, with a new objective or combined with others, in a

that involves new ways of collecting and using data with risk to

the rights and freedoms of people. (…)”

The EDPB develops the definition of DPIA in the WP248 Guidelines as: "… a pro-
process designed to describe the treatment, assess its necessity and proportionality
and help manage risks to the rights and freedoms of natural persons
derived from the processing of personal data, evaluating them and determining the measures
you give to address them."

EIPD is inextricably linked to the principle of proactive responsibility,
to the principle of data protection by design and data protection by default.

Data protection by design and by default is regulated in article 25
of the GDPR.

The principle of privacy by design is an example of the passage from reactivity to
proactivity and the risk approach imposed by the GDPR. Therefore, from the states
God more initial planning of a treatment should be considered this
principle that implies that the person in charge of the treatment from the moment in which
designs an eventual treatment of personal data must protect the personal data
rights and the rights of the interested parties and not only when the
treatment. This is expressed in the CEPD Guidelines 4/2019 regarding article 25
Data protection by design and by default.

The principle of privacy by design is linked to the EIPD as it is a tool
lie to determine and assess the risks of treatment, so that they can
instrument the appropriate technical and organizational measures to avoid ma-
materialization of the risks detected. As established by the Working Group of the
Article 29 in its Guidelines on Protection Impact Assessment
of data (EIPD) and to determine if the treatment «likely carries a high
risk" for the purposes of the RGPD: "The EIPD must be perceived as an instrument to help
in making treatment decisions.

Regarding what interests us now, we will indicate that the EIPD is the responsibility of the

responsible for the treatment, even if it is entrusted to a third party. Temporarily
“should be started as early as feasible in the design of the treatment operation
even though some of the treatment operations are not yet known.” So
determined in the Guidelines on Protection Impact Assessment
of data (EIPD) and to determine if the treatment «likely carries a high
risk” for the purposes of the GDPR.
In addition, it requires the participation of the data protection delegate, since he must control

to carry it out, as provided in article 39.1.c) of the RGPD. In this sense, the
Guidelines on the data protection delegates of the Working Group of the ar-
Article 29, give this figure a relevant and fundamental role by indicating that "if
Guiding the principle of data protection from design, to article 35, section
2, specifically states that the data controller "shall seek the advice-
tion” of the DPD when carrying out an impact assessment related to the protection
of data. In turn, article 39, paragraph 1, letter c), imposes on the DPO the obligation to
«offer the advice that is requested about the relative impact assessment-
goes to data protection and supervise its application in accordance with article
35””. It is important to highlight the recommendation contained in the aforementioned Guidelines in
in relation to the specific functions of the data protection officer in relation to
with the EIPD, since it must verify “if the impact assessment related to the pro-
data protection has been carried out correctly or not and whether its conclusions (if
to go ahead or not with the treatment and what safeguards to apply) are in accordance with

the GDPR".

The lack of EIPD, as well as its defective, incomplete, late implementation or without the participation

cipation of the data protection delegate supposes a violation of the principle of

proactive responsibility and privacy by design, as well as foresight

GDPR provisions on DPIA.

In this case, it was SEDIA that in the Specifications, for the design, develop-

llo, pilot and evaluation of the system, includes a clause (2.1) in which it is established

a series of deliverables among which are the risk analysis or the evaluation

of impact.

As a result, it was mandatory to carry out the EIPD in attention to the elements and

characteristics of the treatment, it is verified the lack of accomplishment in time and form.

In fact, the first version of the EIPD submitted to this Agency was produced in fe-

cha September 22, 2020, by SEDIA. The second version is provided on date

October 30, 2020.

Let us emphasize that the launch of the pilot project in La Gomera has been taking place since

June 29, 2020 through July 31, 2020 and nationwide, commissioning

vice of the application occurs on August 19, 2020.

Therefore, the treatment of the data materialized before elaborating the EIPD, in-

complying with the provisions of article 35 RGPD.

To all this, it must be added that, as has been collected previously, from a

At the beginning, SEDIA stated that no personal data was being processed. This circumstance

evidence shows that there was neither EIPD nor was it planned to be carried out, notwithstanding

However, data processing of a nature was actually being carried out

staff. For this purpose, we must mention that in order to arrive at the affirmation that

there is no processing of personal data, it is mandatory to carry out at least

an initial evaluation of such an extreme to rule it out, an issue that has not been

accredited.

We must also draw attention to the fact that it does not appear in the documentation sent

prior request of the AEPD, any document in which the adviser is recorded.

training and the mandatory participation of the data protection delegate in the EIPD.

Lastly, we will indicate that the subsequent realization of the EIPD does not "correct" the lack of

realization of this in a timely manner and with the participation of all stakeholders

necessary, especially since the lack of risk assessment and adoption

of the appropriate technical and organizational measures, has already produced an intangible damage

in the rights and freedoms of citizens, more reprehensible when the treatment

It is carried out by a Public Administration.

The facts described are constitutive of the infraction foreseen in article 83.4.a)

of the GDPR.

X

The AEPD is aware of the extraordinary and emergency situation that has generated

the COVID pandemic leading to the adoption of multiple measures to put

end the seriousness of the situation.

It is also evident that privacy, the right to protection of personal data

nals, it cannot be an obstacle in the technological advances to combat the pandemic.

mine. As stated in recital 4 of the RGPD: the processing of personal data

it must be conceived to serve humanity. The right to protection of data

personal rights is not an absolute right, but must be considered in relation to

their role in society and maintain a balance with other fundamental rights,

in accordance with the principle of proportionality.

Notwithstanding the foregoing, in this context, we cannot ignore that the primary function

of the AEPD refers to the effective defense of the fundamental right to the protection of

personal data of citizens.

Among the actors involved, the considerable effort made

by the MSND, which through the governing bodies has cooperated favorably

with research, providing a response to the requirements, which is valued

positively.

From what has been exposed so far, it must be concluded that the proven facts violate the dis-

placed in articles: 5.1.a), 5.2, 12, 13, 25, 28.1, 28.3 and 35 of the RGPD, with the scope

ce expressed in the previous Foundations of Law, which, supposes the commission

of the infractions typified in article 83 sections 4.a), 5.a) and 5.b) of the RGPD.

Therefore, in accordance with the applicable legislation, the director of the AEPD RESOLVES-

GO:

FIRST: IMPOSE on the GENERAL DIRECTORATE OF PUBLIC HEALTH the sanction

of WARNING for infraction of the following articles:

- Articles 5.1.a) and 5.2 of the RGPD, typified in article 83.5.a) of the RGPD and in

article 72.1. a) of the LOPDGDD, for the sole purpose of determining the

prescription bolts.

- Articles 12 and 13 of the RGPD, typified in article 83.5.b) of the RGPD and in the

Article 72.1.h) of the LOPDGDD, for the sole purpose of determining the deadlines of prescription.

- Article 25 of the RGPD, typified in article 83.4.a) of the RGPD and in the Article 73 of the LOPDGDD in section d), for the sole purpose of determining prescription periods.

- Articles 28.1 and 28.3 of the RGPD, typified in article 83.4.a) of the RGPD and in Article 73 of the LOPDGDD in sections: k) and p), for the sole purpose of determine the statute of limitations.

- Article 35 of the RGPD, typified in article 83.4.a) of the RGPD and in the article 73 of the LOPDGDD in section t), for the sole purpose of determining prescription periods.

SECOND: NOTIFY this resolution to the GENERAL DIRECTORATE OF PUBLIC HEALTH.

THIRD: COMMUNICATE this resolution to the Ombudsman, in accordance with the provisions of article 77.5 of the LOPDGDD.

In accordance with the provisions of article 50 of the LOPDGDD, this Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with article 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 AEPD within a month from the day following the notification cation of this resolution or directly contentious-administrative appeal before the Contentious-administrative Chamber of the National High Court, in accordance with the provisions placed in article 25 and in section 5 of the fourth additional provision of the Law 29/1998, of July 13, regulating the Contentious-administrative Jurisdiction, in the period of two months from the day following the notification of this act,

in accordance with the provisions of article 46.1 of the aforementioned Law.

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

the firm resolution may be suspended in administrative proceedings if the interest

sado expresses its intention to file a contentious-administrative appeal. Of being

In this case, the interested party must formally communicate this fact in writing

addressed to the AEPD, presenting it through the Electronic Registry of the Agency

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

records provided for in article 16.4 of the LPACAP. You must also transfer to the

Agency the documentation that proves the effective filing of the contentious appeal

so-administrative. If the Agency was not aware of the filing of the appeal

contentious-administrative within a period of two months from the day following the notification

cation of this resolution would terminate the precautionary suspension.

Sea Spain Marti

Director of the AEPD

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es