 File No.: PS/00222/2021

- 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
mo criterion used before any news published in the media
that would affect the processing of health data by the Public Administrations.
cas, and, given the news that appeared in the media regarding the project
of the Government of Spain about the implementation of a tracking application (or App)
treo of possible COVID-19 infected, entrusted to the SECRETARY OF STATE
DIGITALIZATION AND ARTIFICIAL INTELLIGENCE (hereinafter, SEDIA), of the
MINISTRY OF ECONOMIC AFFAIRS AND DIGITAL TRANSFORMATION (in
hereafter, the METD), which will use an application programming interface (in addition,
API) of Google and Apple, a protocol to be interoperable between countries, which is
will launch as a pilot in the Canary Islands at the beginning of June, connecting to the systems
health computer systems of the Autonomous Communities, urges the General Subdirectorate
Data Inspection Commission (hereinafter, SGID) to initiate the preliminary actions
of investigation referred to in article 67 of Organic Law 3/2018, of 6
December, of Protection of Personal Data and guarantee of digital rights (in
hereinafter, LOPDGDD), in relation to the actions carried out by SEDIA, in case
From such facts, indications of infraction in the area of competence of the
the AEPD.

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

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

"1. Investigate whether the RadarCovid application complies with the principles of legality,

loyalty, transparency and proactive responsibility of the RGPD (Art. 5), in accordance with

in accordance with the guidelines of the EDPB (Art. 70 RGPD), to the extent 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 to the AEPD before carrying out the treatment-

processing of personal data (Art. 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

ties of the health authorities of the Autonomous Communities that have completed the pro-

technical processes necessary to integrate the application into your healthcare systems

(Art. 13 and 14 GDPR);

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

data of the treatment and their respective legitimizing bases, in attention to the

provided in section “5. For what and why do we use your data? and “10.

What is the legitimacy for the treatment of your data? of the policy of

emptiness (Art. 13 and 14 RGPD); Y

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

scientific or historical research or statistical purposes in the Privacy Policy

ity (Art. 9.2j and 89.1 RGPD).

2. Order SGAD that treatment operations within the framework of Radar-

Covid comply with the GDPR and the EDPB guidelines; Y

3. Sanction SGAD with a warning when treatment operations

have violated the provisions of the GDPR or the guidelines of the EDPB."

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

sends to the AEPD some complementary allegations based on the following

circumstances:

"1. Incorporate said SUPPLEMENTARY ALLEGATIONS to 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

SECOND: Modification of the data controller

THIRD: Security breach

FOURTH: Data communications to the "EU interoperability gateway"

FIFTH. Modification of the RadarCOVID Privacy Policy

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 sent the Vice President Nadia Calviño and the Secretary of State Carme

Artigas this Monday, 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: C.C.C. (hereinafter, claimant 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 (https://radarcovid.covid19.gob.es , with IP ***IP.1, ***IP.2, ***IP.3, ***IP.4

accessible via CloudFront CDN). Therefore, each time a sub-

get the key from a phone to the endpoint ' /v1/gaen/exposed ' of this server,

it can be inferred that the owner of the phone is COVID-positive. The encryption in-

between the application and the server does not help to hide that information: even if the en-

dpoint and the content of the upload are not observable, the length of the messages re-

will watch for an upload of the TEK key 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, on different dates:

Secure Verification Code Requirement

First

Second

Third

Fourth

Fifth

***CSV.1

***CSV.2

***CSV.3

***CSV.4

***CSV.5

Required date

I lie

Notification date-

tion required

I lie

05/26/2020

08/18/2020

09/18/2020

02/10/2020

10/26/2020

06/07/2020

08/29/2020

09/29/2020

10/13/2020

06/11/2020

In the first request, dated May 26, 2020, the following was requested:

information:

(…)

Regarding the treatments

1.- Information about the specific purposes of the app and the data processing

personal data provided within the framework of the aforementioned app.

2.- Information on the types of personal data that could be collected.

users for these treatments, specifically specifying the

health data, location and identification data, in question. Indicate the character

ter obligatory or voluntary to facilitate them. Storage period planned for

each of the aforementioned data or data types.

3.- About the location data that is collected, information about the treatments

subsequent procedures provided with said data and their purposes. additionally

information on the processes of anonymization and/or pseudonymization applied

two.

4.- Detail of the forecast of use of the app in terms of obligation and al-

cancel:

4.1.- Information on the mandatory use of the App.

4.2.- Information on the compatibility of the App with the different versions

operating systems (ANDROID and IOS).

4.3.- Solutions contemplated for users of incompatible systems

and other operating systems (Windows Mobile, etc…).

4.4.- Measures planned for use by minors and

guarantee.

5.- Provided third-party entities involved in the processing, public and

private. Identification of these and a copy of the contracts/agreements signed by

SEDIA and successive subcontracting.

6.- Information on the planned transfers and identification of the categories of

recipients and legitimizing framework in which they will be carried out

7.- Information on compliance with data protection principles,

mainly from the principle of proportionality, limitation of purpose, as well as

of the minimization of the data collected, according to the intended purposes.

Copy of the reports that reflect the studies carried out in your case.

Regarding data storage and security

8.- Description of the databases or files involved in the process,

both in mobile terminals and in central services and communities

autonomous.

Record structure and description of the contents. Description of the

metadata, IP, port, IMEI, device identification, etc… as well as the

purpose for which the data is used.

Information on whether data relating to diagnostic tests are included

in these databases and are associated with the users of the applications.

Information on the location of the information collection servers and

the entities in charge of managing said servers.

9.- Copy of the risk analysis on the rights and freedoms of users

of the app made on the possible treatment of data and the evaluation of

impact related to data protection to be made on this initiative.

10.- Description of the technical and organizational measures implemented that

guarantee the security of personal data, both from the client

downloaded by users as of the information treated in the part of the

server, including, at least, user management, access control,

access log files (logs), backup and procedure of

security breach management. Information on whether the data is stored

ciphers and, if applicable, type of encryption.

11.- Copy of the analysis and management of security risks in the context of

National Security Scheme.

Regarding the App and APIs of Google and Apple

12.- Copy of the Privacy Policy of the app. Copy of any other

evaluation of the data processing foreseen in the app carried out by its

part to date, if any. 12.- Start-up date

provided for the aforementioned app.

13.- Copy of the technical documentation of both the app and the APIs

used in the development of this that includes information on the structure of

data and processes.

14.- Information on whether said application and the interfaces (API) are code

open and whether such APIs have been audited by a third party

independent national or international entity and its result.

15.- Information about the resources of the mobile devices you access

the app and the purpose of each access. Information provided to the user about

these entrances.

16.- Information about the resources of the mobile devices to which

access the APIs and the purpose of each access. Information provided to

user about these accesses.

17.- Description of the tracking and alert procedure including:

- Description of the tracking procedure. Generation procedure

identifiers, frequency of change, locations in which they are stored

and period of conservation of these in each location.

- Detailed description of the communication procedure to users

who have been close to a user who has been found to be infected,

detailing the information communicated.

- Authorities and/or third parties to whom the identifiers are provided.

- Description of the procedure by which a positive is reported

infected with COVID-19. Who introduces it in the circuit. Description of

procedure that guarantees that it is a positive verified by the

health authorities and not a false positive.

Regarding data transmissions

18.- Description of the data transmissions specifying the networks,

protocols and encryption.

19.- Description of the data frames that are transmitted, structure and

contents. Description of the metadata, IP, port, IMEI, Identification of the

device, location, etc… as well as the purpose for which it is used.

this data and which of them are recorded in the files.

The suspension of administrative deadlines provided for in the Additional Provision

third of Royal Decree 463/2020, which declares the state of alarm

for the management of the health crisis situation caused by COVID-19, in

its section 4 establishes: "Notwithstanding the provisions of sections

above, from the entry into force of this royal decree, the entities of the

public sector may agree with reasons to continue those

administrative procedures that refer to situations

closely linked to the facts justifying the state of alarm, or that

are essential for the protection of the general interest or for the

basic operation of services.

Taking into account the particularly sensitive nature of the data in question,

This Agency considers that this is an emergency case that cannot be postponed, in

which it is necessary to safeguard the fundamental right to the protection of

personal data, so its urgent nature would be undermined if it were seen

affected by the suspension of deadlines decreed (...).

In the second request, dated August 18, 2020, the following was requested:

information:

(…)

1.- Updating of the information and documentation provided regarding the system

RADAR COVID that may have changed from the pilot version.

2.- Copy of the service contracts provided by Amazon Web Services (AWS).

3.- Information on the role played by the Secretary of State for

Digitization and Artificial Intelligence, as well as the Ministry of Health in the

management of the RADAR COVID system, and where appropriate, a copy of the contracts or

agreements signed between the two.

4.- Regarding the treatments carried out by the Autonomous Communities:

• Information on the role played by the Autonomous Communities in

the management of the RADAR COVID system, and where appropriate, a copy of the contracts

or signed agreements.

• Description of the treatments they carry out.

• Detailed description of the procedure established for communication

of the positive identifiers of COVID 19. Copy of the protocols and

documentation about it.

• Description of the information system used by the CCAA for the

management of diagnostic codes.

• Description of the security measures of this system, including the

management of users and passwords (registration and cancellation procedure) and type of

communication encryption.

5.- Regarding data storage and security

5.1.-Description of the back-end databases:

Structure of the database, description of the tables and each

one of the fields.

Printed copy of a complete record of each table including the

description of the contents of the fields.

Information on whether the data is stored encrypted and, if so,

encryption type.

C/ Jorge Juan, 6

28001 – Madrid

5.2.- Copy of the risk analysis on the rights and freedoms of

users of the app made about the possible data processing of

personal nature and the impact assessment related to data protection

make about this initiative.

5.3.- Description of the technical and organizational measures implemented

that guarantee the security of personal data, including the management

of users, access control, access log files (logs), copy

security and security breach management procedure.

5.4- Copy of the security risk analysis and management in the context of

National Security Scheme.

6.- Description of the interoperability procedure with other Apps

developed for the same purpose by third countries.

6.1.- Data that is shared or is planned to be shared by users.

6.2.- Description of the procedure established to share said data.

6.3.- Description of the data collection procedure for

user identifiers of other Apps.

6.4.- Description of the communication procedure to users of other

Apps that have been in contact with positive users. (…)

In the third requirement, dated September 18, 2020, the

Next information:

(…)

1.- Purposes for which Firebase software libraries are used

Google after completing the pilot phase, and in particular those that use the service

Google analytics, as can be seen from the app code recently

made public on hithub.com (On lines 198-199:// Recommended: Add

the Firebase SDK

implementation

'com.google.firebase:firebase-analytics-ktx:17.5.0').(…)

Google Analytics.

for

In the fourth request, dated October 2, 2020, the following was requested:

information:

This Agency has received a document reporting a

security incident detected in relation to the Radar COVID app that

is stated verbatim:

“only COVID positive users upload TEK keys (keys with the

test result) to the radar-covid-backend-dp3t-server, https://

radarcovid.covid19.gob.es/ (with IP: ***IP.1, ***IP.2, ***IP.3, ***IP.4 accessible

via CloudFront CDN). Therefore, whenever a

key upload from a phone to the endpoint of this server

'/v1/gaen/exposed', it can be inferred that the owner of the phone is

COVID positive. The encryption between the application and the server does not help

cover up that information: even if the endpoint and upload content

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

TEK key to the server.

Communication can be observed by various entities. For example,

the telecommunications provider (if the connection is made through

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 appRadar COVID, in which the

Uploads are done using the Cloudfront endpoint that is used for uploading.

downloading the TEKs, Amazon also has the ability to

observe the IP addresses of Radar COVID users and associate them with the

fact that these users report a positive COVID test.

Observable IP addresses constitute personal data as they

"contain information concerning natural persons 'identified or

identifiable'" (the Judgment of the Third Chamber of the

Supreme Court, Section. 6, of October 23, 2014, ECLI:

ES:TS:2014:3896, interpreting the old LOPD). But besides the fact

communicate the IP address, given that, as shown in the

technical report, only COVID positive users upload the keys to the

radar server-covid-backend-dp3t-server, that IP is associated with the

uploaded TEK key data, which always corresponds to the communication

of a positive COVID test.

In this way, the operation of the app allows linking in a way

unequivocal an IP with the fact that its owner is uploading a test

COVID positive. Thus, without the user being aware of it, the

app makes it possible for third parties to know that the owner of an IP is

infected by the virus, which implies the communication of a sensitive data, to the

be a health data (data specially protected according to art.

9 GDPR). While the processing of the IP address is necessary for the

operation of the application, the possibility of associating the IP with the upload

of a positive test is not."

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,

on the protection of natural persons with regard to

processing of personal data and the free circulation of these data (in

hereinafter, RGPD), and Art. 67 of Organic Law 3/2018, of December 5,

Protection of Personal Data and guarantee of digital rights (in

hereinafter LOPDGDD), it is requested that within ten business days, we

inform if they are aware of this fact and, if applicable, the measures

taken for resolution.

In the fifth and last request, dated October 26, 2020, the following was requested:

following information:

(…)

1.- Number of identifiers that have been affected by the vulnerability

dad.

2. Detailed description of the actions carried out to resolve it, including

Going date of the measures adopted and date of their implementation.

3.- Information regarding whether you are aware of the use by third parties

ros of the exposed data.

4.- Communications protocol used between the app and the backend and des-

Detailed description of the type of encryption used. (…)

SEVENTH: In view of the allegations provided by SEDIA in response to the requests

requests made, the SGID issued a report on previous investigative actions

tion within the framework of the file with reference number E/03936/2020, dated

February 26, 2021, by virtue of the investigative powers granted to the authorities

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

General Data Protection, hereinafter RGPD), and in accordance with the provisions

do in 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 when the treatment

ment cannot manifestly be based on a different legal basis.

Certain types of treatment may serve both important reasons for

public interest as well as the vital interests of the data subject, such as

when the treatment is necessary for humanitarian purposes, including the control

of epidemics and their spread, or in situations of humanitarian emergency,

especially in case of natural or man-made disasters.

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 preservation. 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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

20/212

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:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

21/212

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

n.For the management of the RADAR COVID system, INDRA has contracted the

services 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,

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

23/212

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.

either

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

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

(https://sede.mscbs.gob.es/canalesAcceso/oficinas.htm)], or presen-

mainly through the network of help desks in matters of re-

registrations using this request model [links to the registration form

request for the exercise of rights General Regulations for the Protection of

MSCBS Data]

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, it uses the ENS safeguards catalog, implemented by PILAR,

the second also incorporates the catalog of safeguards of the Regulation

General Data Protection (RGPD) implemented by PILAR. From the report

From the risk analysis that incorporates both safeguards, it can be deduced that

Next:

• 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 valuation has been carried out in accordance with the information available

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 list of threats that has been considered for the Risk Analysis.

gos and that constitutes the catalog of threats implemented in a

standard in the PILAR tool are: Natural disasters, of in-

industrial, errors, unintentional failures and intentional attacks.

• 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 one of the articles of the

GDPR that must be taken into consideration.

• The value of the Potential Risk obtained from the PILAR tool is 6.3

out of 10 (Very critical risk). Assets that present a level of risk

critical are: Communications networks, RADAR COVID app, support, installation

AWS connections and AWS equipment.

- The value of the Residual Risk (after applying the safeguards) ob-

score of the PILAR tool is 2.6 out of 10 (measured risk).

it gave). once the safeguards have been taken into account

planted, the risk level of the assets is considerably reduced.

Possibly, there are 12 assets with negligible risk, 1 with

low and 1 with medium risk.

- The value of the Objective Risk (Objective to be achieved after the

proposed safeguards) obtained from the tool

PILAR lie 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 PILAR for the National Security Scheme

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:

- Use qualified certificates for the digital signature used

in the positive verification service.

- Although access to the AWS console is done through 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 related to

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 (temporary exposure keys)

with which the user's device has generated the random codes.

rios or Rolling Proximity Identifier - RPI). These data are communicated

will inform the health authorities only when it has been confirmed

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

tion that the person chooses to do so, that is, in a way

volunteer.

- Data through which the user is previously warned of a contact

to risk These data allow estimating how many users are warned.

due to the application of a potential risk of contagion, without being able to scratch

reveal your identity, and allows the National Health Service to prepare

initiatives and resources needed to serve users who

have received the notification.

- The day the user developed symptoms consistent with COVID-19.

- Code provided by the health authorities to allow the

user activate a warning alert. This 12-digit number will be

provided by the health authorities to the users of the application.

tion using Quick Response code (QR). Users may, voluntarily

regularly, enter said code in the Application to confirm the

positive diagnosis and trigger the notification procedure to

your close contacts. This code is a diagnostic confirmation.

co positive of a user. There is verification of said code to avoid

for any user to submit false evidence.

- The IP address that the device uses to connect to the Internet.

These data do not allow the direct identification of the user or his device.

positive, with studies on the robustness of encryption protocols

tography and anonymization, although there is a possibility that they may

break down and associate the identifiers with phone numbers and per-

sonas, applying sufficient time and computing capacity, although this

is considered highly unlikely. On the other hand, it must be taken into

account that the processing of information not only affects the user of

the application, but also that of all third parties with whom you have been

do 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.

C/ Jorge Juan, 6

28001 – Madrid

- 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.

• A description of the elements involved in each one is made.

of the phases of the life cycle of the treatment data (activity, act-

res and systems).

• A description of the intervening technologies is made.

• 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 "PILAR" tool through which it has been carried out

carried out the evaluation of risks and safeguards for the treatment "Radar

COVID” and all the infrastructure that has been implemented for this service.

vice.

• 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 PILAR for the

National Security Scheme to raise them to the recommended value.

• Conclusions collected 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 (as of the date of the checks carried out by the data inspection)

which was updated on October 29, 2020, in which the following have been carried out:

following 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:

- The app does not require registration as a user, nor does it request character data

staff. The only information requested is the language.

- Reports the functionalities of the application, which works without revealing

the identity of the user or the device. Does not collect name, phone or

geolocation and that you can stop using it at any time.

- Includes a link to the privacy policy, having to accept it to con-

continue Include a link to the terms of use.

- Request permission to activate COVID exposure by activating

bluetooth and to ignore battery optimization and keep running.

running in the background of the app.

- Once the installation is finished, 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.

- 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.

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

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.

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, Den-

brand, Spain, Poland, Latvia and Ireland, as well as the data transmitted by

the APIs of GOOGLE and APPLE, in order to evaluate the privacy of the

users.

Concludes the Trinity College report that analyzed the data transmitted to

back-end servers by implemented contact tracing applications

minted in said countries in order to evaluate the privacy of users

They consist of two independent components: a "client" application managed
reported by the national public health authority and the notification service of
Google/Apple exposure, which on Android devices is managed
by Google and is part of Google Play Services. The client applications
the health authority generally behave well from the point of view
of privacy. However, the Google Play Services component of this
These applications is worrying from a privacy point of view.
Google Play Services contacts the appropriate Google servers.
approximately every 20 minutes, potentially allowing monitoring
of the location with precise products through the IP address. Also,
Google Play services also share the phone's IMEI, the number
hardware serial number, SIM serial number, mobile phone number,

the user's phone number and email address with Google, along with
Detailed data on applications running on the phone. Is
data collection is enabled simply by enabling the services of
Google Play, even when all other Google Play services and settings
Google 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 the authorities
des 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 no-

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 SEDIA, in accordance with the provisions of articles 63 and

64 of Law 39/2015, of October 1, of the Common Administrative Procedure of the Public Administrations (hereinafter, LPACAP), for alleged infringement of the following articles of the RGPD: 5.1.a); 5.2; 12; 13; 25; 28.1, 28.3 and 28.10; and 35, typified in articles 83.4.a) and 83.5.a) and b) of the RGPD.

NINTH: On June 7, 2021, SEDIA presents a document through which requests the extension of the term to submit allegations and provide documents or other elements of judgment, and in addition, the remission of the sanctioning file.

TENTH: On June 8, 2021, the examining body agrees to extend the period requested up to a maximum of five days and dated June 11, 2021, the remittance sion of the copy of the file, in accordance with the provisions of articles 32.1 and 53.1 a) of the LPACAP.

The extension agreement is notified on June 8, 2021, through Folder Citizen.

The referral of the copy of the file occurs on June 14, 2021, via courier, according to the delivery certificate that appears in the file.

ELEVEN: On June 15, 2021, it is presented, in a timely manner, written in the one who adduces allegations and expresses what is appropriate to his right:

In summary, it states that:

GENERAL ARGUMENTS:

The project to build the national contact tracing solution, Radar COVID, has been very demanding due to the very tight deadlines managed (which that imposed contracting by emergency procedure), due to the technical difficulties inherent nology, and the complexity of interoperating with the 19 health systems riors of the Autonomous Communities and Cities, as with other countries of our environment, through the interoperability node of the European Commission.

Despite these difficulties, it was developed very quickly, with technical solvency

and epidemiological, and with the maximum guarantees of data protection, using the

protocol that guarantees privacy (DP3-T), which includes strict considerations

privacy by design, this protocol is used by a majority of countries in

implementation of such applications.

Given the rush of deadlines, a work system of weekly meetings was implemented

them with all the agents involved

-

The Ministry of Health (hereinafter, MSND) and the Canarian Community,

participating in all pilot meetings and being involved in all decisions

strategic decisions that were taken for its development, execution and evaluation.

-

The MSND, present at all these meetings, leading the execution of the

jobs, how could it be otherwise as he is responsible for the National System

National Health Service and giving precise indications throughout the evolution process

of the application from the pilot, through the testing phase to the consolidation

giving of the app

-

The SGAD, executing technological developments and promoting the use of

the application to achieve greater effectiveness of this, always counting on

the necessary coverage to do so, and with a specific mandate in each case

of the MSND as the health authority of the country:

o Letter from the Director of Public Health for the pilot.

o Agreement of the Interterritorial Council of the National Health System for the use

in COVID Radar tests.

o Agreement of October 13 for the definitive use of the application and signature of the

corresponding agreements.

Corresponding to the SGAD in all cases, the role of Treatment Manager,

which is what he has exercised throughout the development and evolution of the application.

Also that technical experts in access have joined the COVID Radar team.

from the ONCE Foundation and CERMI to provide even more trans-

parity all the processes carried out to improve the accessibility of the

application and as external validators of the same.

Unusual transparency measures have been taken in the Public Administration.

Spanish ca as the publication of the Risk Analysis, and the Impact Assessment,

as well as the source code of the application for general scrutiny by professionals and

experts in privacy, security and data protection.

The Impact Assessment document has also been analyzed by the group

eHealth of the European Union, attesting to the privacy of the application and the non-re-

collection of any personal data or data that allows the user to be identified.

In addition, the requests and doubts that the analysts or technicians have

raised on the source code published on Github.

Many parliamentary questions have been answered, questions from the Ombudsman of

People, consultations for the right of access under the Transparency Law, thousands of

questions from users of the application, etc.

Unfortunately, the initiation of preliminary investigative actions by the

AEPD on May 21, 2020 has not allowed the exchange of information.

The SGAD has acted at all times respecting the indications given by the

MSND, always acting in line and with the requirements established in the initiatives

in this matter, and trying, in the exercise of its competences, and

according to the assigned role, respond to the demands that at that time

commanded the citizens acting, within the urgency that the works have required

during the emergency situation, with full respect for all legal requirements

required.

SPECIFIC ALLEGATIONS:

REGARDING REQUESTS FOR INFORMATION FROM THE AEPD

The initiation of investigative actions by the AEPD coincided with the

with the announcement of the contact tracing pilot project in La Gomera, in a mo-

moment in which the work team of the Radar project was not yet constituted

COVID, and therefore the project was not started either, strictly speaking.

For this reason, the first information requirements requested by the AEPD referred to

reference to documents that were not available simply because they did not exist at all.

still, since they were not necessary as they were fictitious data.

The emergency contract entered into between the SGAD and INDRA begins on June 15.

child of 2020.

In view of the allegations of the SGAD in response to the requirements of the

AEPD, dated February 26, 2021, the SGID issued a report on actions

prior investigation.

This report investigates: SEDIA, and the General Secretariat of Digital Health, In-

Training and Innovation of the National Health System of the MSND.

The health authorities of the Autonomous Communities are not investigated, even

when the Agreement of August 19, 2020 of the Interterritorial Health Council on

the use of the Radar Covid application, in the testing phase, by the Communities

des and Autonomous Cities, indicates its competence as responsible for the treatment

of data in their respective territory.

Likewise, the text of the Agreements signed between the SGAD and the Ministries of

Health of different Autonomous Communities, it can be deduced that the latter have

co-responsibility in the processing of data, in particular those related to tracking

of automated contacts, such as the management of the confirmation codes of

site.

REGARDING THE PROCESSING OF PERSONAL DATA

The Radar COVID application performs certain data processing, such as: identification-

ephemeral data (pseudonymized data) or 12-digit position statement code

tive.

It is an application that follows the DP3-T protocol, privacy protection by di-

design, using the exposure notification system that Apple and Google announced

cialized on April 10, 2020, and used in 19 countries of the European Union to

build your contact tracing apps.

Therefore, it was initially alleged that there was no processing of personal data.

It is also necessary to remember that the application does not register users, nor does it obtain

has information on the mobile device, nor does it geolocate, nor does it collect the IP address of the device.

moving positive. It only requires bluetooth communications to exchange codes

random (ephemeral bluetooth identifiers) that do not reveal the identity of the user

of the application and that are always between two mobile terminals and with the prior con-

user sentiment.

In any case, the SGAD sent, at the time, the conditions of use and policy of

privacy of the application to the AEPD, requesting that they review and provide ob-

servations. Given that the Agency was already acting in the procedure for updating

previous tions, there was no possibility of such a report, a situation that has continued in the

time so far.

Additionally, in the period from June 29 to July 29, the application was operative

tive for a pandemic simulation pilot on the island of La Gomera. The relative data

The declaration of positive cases for COVID-19 were completely simulated,

as evidenced by the terms of use and privacy policy at that time.

unto

At a later time, the privacy policy is updated to collect the treatments

data processing in relation to:

1. Temporary exhibition keys.

2. 12-digit codes for declaration of positives.

3. User consent to send passwords.

There are other data, such as IP addresses, which, although they can be obtained, are not

are processed. This is expressly stated in the privacy policy.

Finally, it is indicated that the application does not perform a user registration, nor does it obtain

mobile device training.

Notwithstanding all of the above, it is not ruled out that in the future they may be carried out, for

Competent Bodies, analysis of aggregated data on the volume of discharges

gas of the application, volume of infected users, or other anonymous indicators and

aggregates, for scientific research projects, always complying with the regulations

It's about data protection.

Note, finally, in this section, that regarding the processing of data from the app,

No notice has been received, due to its hypothetical misuse, from the Protection Delegates.

tion of Data from the Ministries of Health, and of Economic Affairs and Transformation

Digital tion.

REGARDING THE ROLE OF THE SGAD IN DATA PROCESSING

For reasons of clarity, it is convenient to distinguish two stages:

1st. The stage in which the SEDIA pilot project is carried out was authorized on the 9th of

June 2020 by the DGSP of the MSND to conduct a pilot project on the island of Go-

mere, which allowed the completion of the corresponding contract file.

The contract included the design, construction of the application, the achievement of a

pilot, and its evaluation, as well as adaptations of the application based on

the pilot results. The contract was made for a duration of five months, until

on November 14, 2020

In its authorization, the DGSP establishes on June 9, 2020 that: the person in charge of the

treatment of the data of this pilot will be the health authority of the Community in

that is going to be carried out.

SEDIA remains in charge of processing the data and results.

The DGSP participated in the weekly meetings of the pilot, for the formation of the

goals and means of the project. In particular, D, X.X.X., Director of the Coordination Center and Health Alerts, as well as personnel from his unit, were part of the follow-up weekly lie. Authorities were also part of the follow-up committee. health of the Government of the Canary Islands, and responsible for the Digital Modernization area.

In any case, the data handled in the pilot carried out between the months of July January and July 2020 only handled simulated infection data, not putting themselves in compromise any personal data, much less related to the health of the pilot participants. The project team, together with independent experts have published an article on the work carried out in San Sebastián de la Gomera in the journal Nature Communications, giving an idea of the usefulness of this tool to effects of cutting virus transmission chains: “A population-based controlled experiment assessing the epidemiological impact of digital contact tracing”, see https://www.nature.com/articles/s41467-020-20817-6

2º.- The stage in which the application is launched in the testing phase and posteriorly the ultimate app.

The Agreement adopted on August 19, 2020 in the Interterritorial Council of the System National Health, noted that:

“During the term of this Agreement, the data controller will be the MSND and, in their respective territory, each of the Communities and Cities Autonomous that are incorporated during the testing phase to the use of the application, fully displaying its powers in health matters. The in charge of the treatment will be, in both cases, the Secretary of State for

Digitization and Artificial Intelligence.”

This Agreement allows the Autonomous Communities to temporarily assume, until the signature of the aforementioned agreements, the management of the positive diagnosis codes that are assigned to those citizens with a positive PCR test.

Subsequently, 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 Ra-give COVID.”

In this Agreement, the SGAD is empowered to sign Agreements with Communities Autonomous Cities and Authorities, specifying that: “in the aforementioned Agreements of collaboration, the Ministry of Health and the Ministry responsible for health Community or Autonomous City in question will appear as the responsibility responsible for the processing of personal data and the SGAD as the person in charge of processing treatment.”

In the different Agreements, which have all the legally required authorizations gibles, held between the MSND and the Autonomous Communities, it has been pointed out repeatedly rarely that:

“The Ministry of Health is Responsible for the Processing of data from the application. Radar COVID tion. In this condition, among others, the following apply: following treatment activities:

a) Request from the SGAD, as required, the confirmation codes of the sitive by test.

b) Provide the above confirmation codes to users with a diagnosis. positive prognosis”.

Corresponding to the SGAD, among other functions, that of …….”h) Comply with

the tasks as in charge of the treatment indicated by the Ministry of

Health as responsible for it".

Therefore, it is fully accredited that at all times the SGAD acted and acts

solely and exclusively as in charge of the treatment, while the MSND and Comun-

Autonomous entities were and are responsible for said treatment.

It should be noted that at no time has the MSND failed to comply with its obligations

in the Radar COVID project, and has provided guidelines, such as the collections

in the technical document: "Implementation procedure of the App Radar CO-

VID as a complement to manual contact identification systems", coordinates

dinated by the Center for the Coordination of Health Alerts and Emergencies, Directorate

General Public Health, Quality and Innovation and approved by the Alerts Report

and Preparedness and Response Plans.

In addition, as has been seen in the general allegations, at all times

both in the development of the pilot, and in the use of Radar COVID in tests, as

In the Agreement of October 13, the roles of data controller were defined.

treatment and treatment manager, so there can be no doubts about the legitimacy

training that each one had in the development of the application.

Likewise, the reference to the MSND on page 84 of the Initial Agreement is striking.

Sanctioning Procedure: "If the Ministry of Health had wanted to find

recommend to SEDIA the development of the Radar COVID App, would have shown its willingness

tad unequivocally. And I would have done it in the same way as the rest of the encounters.

midas. However, this did not occur."

This statement does not take into consideration that the encomienda, article 11 of the Law 40/15 cannot affect the competence or its exercise, given that the Ministry and the SEDIA may relate through any other instrument or means permitted by current regulations in the public interest, article 9 of the aforementioned law that allows delegate your exercise.

REGARDING THE ROLE OF INDRA

1.- The AEPD points out that “it is not justified why INDRA offers sufficient guarantees as data processor”:

At no time, the specifications for the design, development, pilot and evaluation Implementation of a system that allows contact tracing in relation to the pandemic caused by Covid-19 indicates that INDRA is in charge of the treatment, such a role SGAD has always played it.

It must be remembered that in the Report justifying the contracting file, provided a justification for the advisability of contracting INDRA for its experience experience in technological projects.

Specifically, it cites:

“In order to immediately carry out the development of this System, it is necessary to It will consist of a multidisciplinary team, which collects profiles with functional knowledge nal on contact tracing, mobile solutions architects, specialists in user experience, test technicians and cybersecurity. It has been considered that the company INDRA SOLUCIONES TECNOLOGÍAS DE LA INFOR-MACIÓN, S.L.U., which stands out for its extensive experience in all types of pro-technological projects, as well as in the design of mobile solutions in relation with the COVID-19 health crisis (COVID MONITOR, App C19-Pass), it is technically and organizationally prepared to carry out this project and has

the ability to assemble a team with the required profiles immediately

in order to carry out the tasks and actions to achieve the objectives

of the development project.

INDRA is a multinational company with extensive experience in projects with the

Public Sector, and gathers sufficient guarantees to satisfy the object of the contract. Of

In fact, INDRA periodically submits to independent audits for the certification

tion of its management and production systems in accordance with the main standards

international res, among which are those listed in Annex I.

2.- On the other hand, the AEPD indicates in its report that "if (SEDIA) had acted

in the capacity of data processor [...] should have required the data controller

subject to processing the prior authorization required by the RGPD in writing, before

resort to another person in charge (INDRA) to develop the entrusted service".

On the one hand, SEDIA has always acted as data processor.

Contracting in favor of INDRA includes in the clauses duties in terms of pro-

protection of personal data:

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

Protection of Personal Data and guarantee of digital rights, adapted

ted to Regulation (EU) 2016/679 of the European Parliament and of the Council,

April 27, 2016, and by which Directive 95/46/CE (Regulation

General Data Protection), including the provisions of the additional provision

first of the Organic Law 3/2018, of December 5 and in the Royal De-

decree 3/2010, of January 8. Pursuant to the first additional provision of the
Organic Law 3/2018, of December 5, on Security Measures in the field
of the public sector, the security measures to be applied in the framework of the treaties
Personal data processing will correspond to those of the Administration
of public origin and will be adjusted to the National Security Scheme.
INDRA INFORMATION TECHNOLOGY SOLUTIONS will be required to
S.L.U. the express manifestation of submission to national regulations and
the European Union in terms of data protection in accordance with the articles
35.1d and 122.2 of the LCSP modified by article 5 of the Royal Decree Law
14/2019, of October 31, by which urgent measures are adopted for reasons
public security measures in matters of digital administration, contracting of
public sector and telecommunications."

And in any case, the SGAD informed the MSND about the contracting of the developments and the operation of the system to the company INDRA, and therefore the MSND was aware from the first moment of this hiring and did not raise any objection.

REGARDING THE IMPACT ASSESSMENT RELATIVE TO THE PROTECTION OF DATA.

First of all, it is worth mentioning that although the EIPD published in September 2020 was version 1.1, a version 1.0 of the EIPD already existed prior to August 19, 2020. The EIPD provided to the AEPD was version 1.1, since it is the one that was published, with the deployment in September 2020 of a version of the application, with support bearing of co-official languages.

During the period from August 19 to publication in September 2020, there was an internal debate about the advisability or not of the publication of said document. ment.

The earnest request of the European Committee for Data Protection (hereinafter,

CEPD) does not in itself constitute an obligation to publish this information,

although it does constitute a strong recommendation. In fact, the General Administration

of the State (hereinafter, AGE), which is the sole legal entity, which holds the

adition of responsible and in charge of the treatment through different bodies, not

has been publishing, neither the EIPD, nor the Risk Analysis on which they are based.

The SGAD sought criteria from the METD's data protection delegate. His judgment was

that, in general, these documents should not be published.

In any case, the recommendation of the CEPD was finally followed, and proceeded to publish

Carry out the EIPD and the previous Risk Analysis in September 2020.

REGARDING THE TERMS OF USE AND PRIVACY POLICY

1.- The AEPD indicates in its report that:

“In the first version of the App planned for the Pilot Program on the island of

La Gomera (July 2020) the information was collected in two different documents

regarding privacy.[..] However, none of them defined who was the

responsible or in charge of the treatment”

It should be remembered that the first version of the App (pilot) was used for testing purposes.

bar

aspects such as usability, perception of privacy, and effectiveness of the solution in a

simulated environment. In no case were the health data of the participants handled.

in the pilot.

And the privacy policy included the following notice:

“The USER of this application is warned that when downloading the application

tion on your mobile device and using it, you are merely participating voluntarily

mind in a PILOT EXPERIENCE WITH FICTITIOUS DATA alert of

COVID-19 infections on THE ISLAND OF LA GOMERA.

It is also reported that this application will stop working once

complete the pilot experience.

Therefore, in the use of the application, all notifications of exposures to

possible contagion of the disease that the user may receive correspond to

simulated assumptions and, for the same reason, as it is a pilot experience,

lotto with fictitious data, suggestions for adopting preventive measures and

care providers who, after this notification, provide the application have no other value.

need to check that the application is capable of providing suggestions of that

type to a user who received a notification of exposure to possible contact

gio"

2.- On p. 110 of the agreement states that: "On the other hand there have been various

revisions to existing ‘Terms of Use’ and ‘Privacy Policy’.”

The Radar COVID team has been reviewing and updating the documents with the

encouragement to improve its content and make it easier to read and understand. Additionally, it

they have incorporated additional issues such as European interoperability.

With each update of the application, if there was a change in the conditions of use and possible

privacy policy, express consent was requested again from the users.

users.

3.- On p. 111 mentions that “it is not clear who is responsible for the trafficking

neither the data of the DPD, which is not even mentioned in the policy of

privacy".

The current privacy policy (https://radarcovid.gob.es/politica-de-privacidad) is

establishes the MSND and Autonomous Communities as data controllers, and

as in charge of the treatment to the General Secretariat of Digital Administration.

4.- Regarding the increase of 700 words in the privacy policy, the SGAD has

been revising the documents with the aim of improving their content and facilitating their reading.

ra and understanding. It corresponds to more extensive explanations of the sections

of privacy, as well as the extension to new uses of the application, such as the inter-

compatibility with European Union contact tracing applications.

The new functionalities (such as the connection of Radar COVID to the European node of

interoperability) has led to the updating of the conditions of use and policy

of privacy, in order to provide transparency and information to users of

the application.

5.- Regarding the information indicated in the terms established in articles 12

and 13 of the RGPD:

The conditions of use and privacy policy have always been accessible to

those interested, both from the mobile application and from the web http://radarcovid.-

gob.es

Therefore, express consent to these two documents is necessary in order to

use the app. In the time that the application is operational, SEDIA has not received

received any complaint from the Data Protection Delegate of the MSND in relation to the

COVIDRadar application.

6.- About the information related to the person in charge, recipients or the rights of the ar-

titles 15 to 22:

Just remember that in the privacy policy there are links to both a form of

the AEPD for the exercise of rights, as well as a link to the MSND, to contact

with the Data Protection Delegate.

REGARDING THE DETECTED VULNERABILITY (COMPLAINTS 2 AND 3)

The vulnerability reported by a group of privacy experts was received at

mid-September 2020. The vulnerability was analyzed and an update was scheduled.

correction coinciding with an upcoming release of the application. It was corrected on 8

October 2020, and shared the code that corrected the issue with the team

technician of the Federal Polytechnic School of Lausanne (EPFL), which is the one who had im-

pressed the DP3-T protocol, guarantor of privacy.

Likewise, it has not been detected nor is there evidence that this theoretical vulnerability

has been exploited or taken advantage of in any real case, surely due to the difficulty

and little benefit that would be obtained from its implementation.

There is no 100% secure system, and it was decided to continue, since the alternative

was to paralyze the use and development of the app with the consequent risk in its full state

health emergency alarm.

REGARDING THE DOCUMENTARY SOURCES USED BY THE AEPD

The press releases have a merely informative value of a public performance and

not attributive of any competence, reserved this attributive power to the rules

and acts mentioned in the previous allegations of this document.

Therefore, we consider that they cannot be given the value described in the AGREEMENT.

DO OF USE OF THE “RADAR COVID” APPLICATION, IN THE TESTING PHASE, BY

PART OF THE AUTONOMOUS COMMUNITIES AND CITIES of the Interterritorial Council

torial of the National Health System (August 19, 2020), the Resolution of October 13,

October 2020, of the Undersecretariat, by which the Agreement between the Ministry

of Economic Affairs and Digital Transformation and the MSND, about the application

"Radar COVID (BOE of October 15) or the different Agreements signed between the

SGAD and the Autonomous Communities and published in the BOE.

In all of them, the role of SEDIA is included: The person in charge of the treatment will be, the Se-

Secretary of State for Digitization and Artificial Intelligence.

CONCLUSION

The SGAD considers that there has been no infringement of the precepts mentioned in the

FIRST section of the AGREEMENT TO START THE SANCTION PROCEDURE-

DOR, and therefore the start of this procedure is not appropriate.

On the other hand, if the resolution derives from measures that have to be adopted for the

better compliance with data protection regulations, there is a strong will

by the SGAD to proceed in this direction, following, in any case, the directions

AEPD guidelines and guidelines.

These allegations have already been answered in the motion for a resolution and are reiterated,

in part, in the Legal Basis (hereinafter FD) of this Resolution.

TWELFTH: On September 22, 2021, the instructor of the procedure

agreed to perform the following tests:

1. Claims filed by

a C.C.C., A.A.A., B.B.B. and RIGHTS INTERNATIONAL SPAIN, and the documentation

tion that accompanies them.

2. The documents obtained and generated by the Inspection Services before the SE-

CERTIFICATE OF THE STATE OF DIGITALIZATION AND ARTIFICIAL INTELLIGENCE (SE-

www.aepd.es

sedeagpd.gob.es

C/ Jorge Juan, 6

28001 – Madrid

59/212

DIA) and the GENERAL DIRECTORATE OF PUBLIC HEALTH (DGSP), and the Action Report

previous situations of the General Subdirectorate of Data Inspection that form

part of file E/03936/2020.

3. Likewise, the allegations to the agreement are considered reproduced for evidentiary purposes.

initiation document PS/00222/2021 presented by SEDIA, on June 15,

2021, through the Reg. Aux. of the Secretary of State for Public Administration.

4. SEDIA 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:

a) Total number of app users who participated in the pilot phase

and total number of pseudo-random codes or proximity identifiers.

ity that were uploaded to the server during this phase.

b) Information on the data collected through the pilot application (in-

including connection data between the user's terminal and the server and the

metadata).

c) Information on the processing of personal data, understood as the

set of operations performed on that data.

d) Information on the following question: What did the material materially consist of?

that data processing?

Specifically, the life cycle of the processed data, the process of these dis-

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 provide-

be in its initial version, together with any additions, modifications or exclusions

sion in the content of this.

f) Copy of the impact assessment related to data protection respec-

to the pilot project and related documentation. Specification of the su-

object that elaborates it and the moment in which it is carried out (start and end date).

zation).

g) If the Impact Assessment was prepared, supporting documentation of the

participation of the data protection officer in it.

h) Copy of the impact assessment, version 1.0, to which it refers in

the allegations (page 20).

i) Documentation accrediting the participation of the protection delegate

of data in the impact evaluation version 1.0.

j) Data protection risk analysis on the pilot project and documents

mention relating to it. Specification of the subject that prepares it and the

moment in which it is carried out (start and end date).

k) Copy of the content of the minutes of the meetings held between the SE-

DIA and the General Directorate of Public Health, Quality and Innovation, or another

higher or directive body of the Ministry of Health, which include the information

information regarding agreed decisions on the protection of data

applicable to the pilot project, with identification of the condition of the

different participants (responsible or in charge).

l) Copy of the content of the minutes of the meetings held between the SE-

DIA, the Ministry of Health (or its superior or directive body) and the

Autonomous Community of the Canary Islands, on the project for the application of

Radar COVID, which include information regarding the decisions agreed upon

data protection measures applicable to the pilot project.

m) Documentation accrediting the contract or other legal act signed between

the General Directorate of Public Health, Quality and Innovation or another body

superior or director of the Ministry of Health and SEDIA, to carry out

pilot project, in accordance with the provisions of article 28.3 of the Re-

regulation (EU) 2016/679, of April 27, 2016.

n) Documentation accrediting the documented instructions of the Di-

General Directorate of Public Health, Quality and Innovation or another subordinate body

superior or director of the Ministry of Health, addressed to SEDIA, in accordance with

to the provisions of article 28.3.a) of Regulation (EU) 2016/679, of 27

April 2016.

o) Documentation accrediting prior authorization, in writing, specifically

or general, in favor of SEDIA or the General Secretariat of the Admi-

Digital Administration (SGAD) by the General Directorate of Public Health

ca, Quality and Innovation or another higher or directive body of the Ministry of

Health, in relation to the contract signed with INDRA, in accordance with the provisions

placed in article 28.2 of Regulation (EU) 2016/679, of April 27,

2016.

p) Copy of the specifications of administrative clauses and technical requirements

cas, if any, and a copy of the manager or sub-manager contract

of the treatment signed between SEDIA or SGAD and INDRA, in relation

with the pilot project.

q) 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.

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

further development to 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:

a) Personal data required by the Radar COVID application to function

operate correctly and fulfill its purposes.

b) Information on the processing of such personal data, understood

as the set of operations performed on that data.

c) Information on the following question: What has the material-

Mind that data processing?

Specifically, the life cycle of the processed data, the process of these dis-

from its collection to its deletion or blocking.

d) Documentation accrediting whether the protection delegate has been requested

tion of METD data advice on the legal nature of the

processed data and the response, if any, that it has formulated.

e) Copy of the record of personal data processing activities

made in the Radar COVID application. This record, referred to

Article 30 of Regulation (EU) 2016/679, of April 27, 2016, must-

will be provided in its initial version, together with any additions, modifications

or exclusion in the content of this.

f) 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 ME-

TDy the Ministry of Health, about the application "Radar COVID".

The notification of the agreement was made on September 22, 2021, by means of

of the Electronic Notifications Service and Authorized Electronic Address, according to

certificate in the file.

THIRTEENTH: On October 25, 2021, SEDIA submits a letter to

through which he requests an extension of the test period to ten working days

them more.

The agreement that grants an extraordinary trial period, for a period of 10 days,

It is notified on October 28, 2021 through the Electronic Notification Service.

nicas and Electronic Address Enabled.

FOURTEENTH: The SEDIA, dated November 22, 2021, in response to the

notified evidence requirement provided the following documents to the proceedings:

cough:

- Answer and remittance of documentation in the trial period of the procedure.

sanctioning action of the AEPD in relation to the Radar COVID application.

- Doc. 1. Radar Covid Conclusions Report of January 28, 2021

- Doc. 2. EIPD Report_ COVID Radar v.1.0.pdf

- Doc. 3. AARR_AppCOVID_v1.0.pdf

- Doc. 4. MINUTES OF THE MEETING OF THE INTER-TERRITORIAL WORKING GROUP Vi-

deoconference June 17, 2020

- Doc. 5. COVID RADAR PRESENTATION GENERAL OPERATION JUNE

2020

- Doc. 5 bis. PILOT PRESENTATION TO CCAA'S JUNE 2020

- Doc. 6. PRESENTATION COVID RADAR MONITORING 07-17-2020

- Doc. 7. MEETING MINUTES JULY 21, 2020

- Doc. 8. PRESENTATION COVID RADAR MONITORING 07-24-2020

- Doc. 9. MEETING MINUTES JULY 27, 2020

- Doc. 10. MINUTES OF AUGUST 5 MEETING **

- Doc. 11. COVID MONITORING RADAR PRESENTATION JULY 31, 2020

- Doc. 12. PRESENTATION AUGUST 21, 2020

- Doc. 13. MINUTES AUGUST 26, 2020

- Doc. 14. Mandate of the General Directorate of Public Health of the Ministry of Health.
giving its approval for the development of the mobile application pilot for the
traceability of COVID-19 contacts

- Doc. 14 bis. AGREEMENT BETWEEN THE METD (SECRETARIAT OF STATE FOR
TALIZATION AND ARTIFICIAL INTELLIGENCE) AND THE MINISTRY OF HEALTH
ABOUT THE “COVID RADAR” APP

- Doc. 15. Specifications for the design, development, pilot and evaluation of a system that
allows contact tracing in relation to the pandemic caused by covid-
19.

- Doc. 16. Press release JUNE 23

- Doc. 17. Press release AUGUST 3

- Doc. 18. Press release SEPTEMBER 9

FIFTEENTH: On January 26, 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 SECRETARIAT OF STATE FOR DIGITAL
ZATION AND ARTIFICIAL INTELLIGENCE, 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.

- Article 28.3 of the RGPD, typified in article 83.4.a) of the RGPD and in the

Article 73 of the LOPDGDD in section k), for the sole purpose of determining

prescription periods.

- Article 28.10 of the RGPD, typified in article 83.4.a) of the RGPD and in the

Article 73 of the LOPDGDD in section m), for the sole purpose of determining

set 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 27, 2022, through the Electronic Notifications Service and

Electronic Address Enabled, the resolution proposal is notified.

SIXTEENTH: On February 7, 2022, SEDIA requests an extension of the

term to formulate allegations to the proposed resolution.

SEVENTEENTH: On February 7, 2022, the examining body agrees to-

Reasonably deny the request for an extension of the requested term.

EIGHTEENTH: On February 10, 2022, the director of the SGAD, by indi-

cation of SEDIA, presents the arguments to the proposed resolution and attaches

a letter requesting the practice of the test.

In the pleadings, in summary, he argues that:

I. BACKGROUND

When the director of the AEPD urged the start of preliminary investigation actions

(May 21, 2020) nor was the RADAR project work team constituted

COVID nor was the project started in the strict sense, so at that time

(May 2020) there were no “facts” that could be examined.

The requirements were answered in a timely manner, providing abundant ex-

applications, information and documentation, which demonstrates the permanent will

collaboration of SEDIA in the context of the open procedure.

These ex officio actions are carried out three and a half months before the existence of the

first claim, the so-called “claimant party one”.

II. ALLEGATIONS.

It considers reproduced those made throughout the processing of the file, as well as

as the documentation sent during the trial period and previous actions.

A) Regarding the ARGUMENTS OF A GENERAL NATURE:

It argues that RADAR COVID is an App that was created as an additional tool

to help deal with the serious and exceptional health emergency situation

taria in Spain caused by the coronavirus.

In Royal Decree 463/2020, of March 14, essential measures were issued

to deal with the situation, which were proportionate to its extreme gravity

and they did not imply the suspension of any right.

In this context, SEDIA, as the person in charge of treatment, acted in accordance with the

indications given at all times by the MSND, as delegated authority of the Government

government in matters of Health and in matters of public health and as responsible for the treatment of the RADAR COVID application.

It is true that these indications were not reflected in a contract as envisaged in article 28.1 a) of the RGPD and this is so because the state of alarm made it difficult to form lization of the usual instruments provided for in the legislation for these cases under normal circumstances. Yes it is accredited, however, in the documentation provided in the trial period, the holding of a series of meetings to which representatives of the MSND, SEDIA and the company awarded the contract attended. emergency contract for the development of the pilot and the RADAR COVID application, meetings in which the necessary decisions were made to advance in the development development of the pilot and the application.

The protection of health in a context of pandemic determined the need for action act rapidly in a coordinated manner with the collaboration of all the agents involved. and the relationship between the data controller and the data processor occurred in a more agile way, as the circumstances demanded, but no less efficient for that neither less respectful with the right to the protection of personal data nor the respect for the principle of legal certainty

In addition to regular meetings, the METD, through the SGAD dependent on the SEDIA, as the person in charge of the treatment, maintained very frequent contact with the MSND, to receive your indications and to be both departments aligned in the achievement of the common goal.

Thus, the MSND, through the General Director of Public Health, Quality and Innovation tion, gave its approval for the development of RADAR COVID, and SEDIA put everything its commitment to its implementation in the shortest time possible, without detriment to any right. SEDIA always acted motivated by reasons of public interest and if following the indications of the Government and its delegated authority (the Minister of Health)

ty) to help tackle the emergency.

Spain, like other neighboring countries, through SEDIA and the

SGAD, developed under the tutelage of the MSND and in cooperation with other members of the

European Union and the eHealth network, the RADAR COVID digital tool, taking advantage of

do the results of the pilot experience developed on the Island of La Gomera.

B) Regarding the SPECIFIC ALLEGATIONS:

B.1 Regarding the processing of personal data.

The right to data protection, like any other right, is not absolute. Nope

it suffices to abide by the literal application of a norm, without appealing to, or taking into account

its spirit and purpose as prescribed in article 3 of the Civil Code.

The requirement and application of data protection regulations, in certain circumstances,

such special and atypical circumstances, and without prejudice to respect for the principle of legal certainty.

says, it must be balanced and considered. At no time do the responsible agencies

data protection rules can act as if the state of alarm had not

existed or did not affect the matter of its competence and the exercise of its powers.

In the testing phase, SEDIA points out that the data collected and generated by the

application do not allow, by default, the direct identification of the user or his device.

site. However, although, according to recital 30 of the RGPD, users

could become identifiable by associating some online identifier.

nea facilitated by the device or other type of tools or protocols, in the project

pilot data were not real (they were test) and the infected codes for their

introduction in the App were false. When the App was opened in La Gomera to the public,

people could not enter real data of being infected.

The treatment of this data by RADAR COVID has been lawful, it is worth reminding this

Regarding the AEPD Report 17/2020, of March 12, that the RGPD provides that the

legal basis that grants legality to this type of treatment (beyond the cases in which

where the interested party gives consent), we find it in articles 6.1.d)

(when necessary to protect the vital interests of the data subject or other persons

physical) and 6.1.e) (when necessary for the fulfillment of a mission carried out).

in the public interest).

B.2 Regarding the role of the SGAD in data processing

1st. The stage in which the pilot project is done.

On June 9, 2020, SEDIA received the approval of the General Directorate of Health

Public Ministry of the MSND to conduct a pilot project on the island of La Gomera, which could

made it possible to carry out the corresponding contracting file. In your authorization

tion established that: On the other hand, we understand that the data controller

of the data of this pilot will be the health authority of the Community in which

will carry out. SEDIA being in charge of data processing and

results.

The MSND, through the DGSP, participated in the weekly pilot meetings for the

conformation of the aims and means of the project. In particular, D, X.X.X., Director of the

Health Alerts and Coordination Center, as well as staff from its unit, trained

They were part of the weekly follow-up. They were also part of the follow-up committee

health authorities of the Government of the Canary Islands.

In any case, the data handled in the pilot carried out between the months of July

January and July 2020 were simulated infection data (not real data), not putting

compromise any personal data, much less related to the health of the

participants. The project team, together with independent experts, has published an article on the work carried out in San Sebastián de la Gomera in the magazine Nature Communications, giving an idea of the usefulness of this tool in order to cut virus transmission chains.

2º.- The stage in which the application is launched in the testing phase and posteriorly the ultimate app.

The Agreement of the Interterritorial Council of the National Health System, of August 19

of 2020, allowed the Autonomous Communities to temporarily assume, until the signing of the aforementioned agreements, the management of the positive diagnosis codes that were assigned to those citizens with a positive diagnostic test for active infection (PCR or other techniques).

On the other hand, on August 25, 2020, after the meeting of the Council of Ministers, the The President of the Government presented the roadmap to deal with the rise of the "second epidemiological curve", in the context of the SARS-C0V2 pandemic in our country. Among other measures, he cited the strengthening of digital means of tracking, requesting citizens to use RADAR COVID.

Subsequently, the Agreement of October 9, 2020 was published, which empowered the SGAD for the signing of Agreements with Autonomous Communities and Cities, specifically stating that: "in the aforementioned collaboration agreements, the Ministry of Health and the Ministry responsible for health in the Community or City.

Autonomous entity in question will appear as responsible for the treatment of

personal data and the SGAD as the data processor.”

In the different Agreements, which have all the legally required authorizations

gibles, celebrated between the SGAD and the Autonomous Communities, it has been pointed out repeatedly that: “the

Ministry of Health is Responsible for the Data Processing of the RA-

GIVE COVID. In this condition, the following activities, among others, correspond:

from treatment:

a) Request from the SGAD, as required, the confirmation codes of the

sitive by test.

b) Provide the above confirmation codes to users with a diagnosis.

positive prognosis”.

Corresponding to the SGAD, among other functions, that of (...): ”h) Comply with the co-

inserted as in charge of the treatment indicated by the Ministry of Health

as responsible for it”.

It is fully accredited that at all times and in accordance with the instruments

legally binding acts, that the SGAD acted and acts solely and exclusively

as in charge of the treatment, while the MSND and the CCAA were and are the

responsible for said treatment.

In this sense, the MSND has provided guidelines to SEDIA-SGAD, such as

example those included in the technical document called “Implementation procedure

ration of the RADAR COVID App as a complement to manual identity systems

tification of contacts”, coordinated by the Center for the Coordination of Alerts and Emer-

Health agencies, General Directorate of Public Health, Quality and Innovation and appro-

supported by the Report on Alerts and Preparedness and Response Plans.

In this sense, RADAR COVID has been prepared following the epidemiological criteria

cos of the "Strategy for early detection, surveillance and control of COVID-19" published

by the Ministry of Health.

At all times, both in the development of the pilot on the Island of La Gomera, and in the

use of RADAR COVID in tests by the Autonomous Communities, and in its use after said phase of

tests, the roles of data controller and data controller were defined.

treatment. The documents that prove this are:

a) The letter of June 9, 2020 from the General Director of Public Health, California

ity and Innovation giving the go-ahead to the realization of the App.

b) The Agreement of the Interterritorial Council of August 19, 2020.

c) and the Agreement published in the BOE on October 15, 2020.

Regarding the statement contained in the proposal on page 159: “The AEPD does not understand

neither to examine nor to qualify what should be the legal instrument through which

formally entrusts SEDIA with the commissioning of the treatment referred to the requested project.

loto RADAR COVID (...)”, SEDIA refers again to the documents indicated

previously.

The AEPD makes a lengthy reasoning to point out that, in its opinion, the SEDIA has played

do, clearly, the role of data controller, but in the documents that are

have cited, SEDIA always appears with the person in charge of the treatment and its actions

have always been aimed at fulfilling this function.

It also alludes to the value of the METD Press Releases, which the AEPD grants in the

page 140: “Press releases raise transparency and accountability to their

maximum expression and are included as part of the proven facts for this reason.”

SEDIA can only disagree with this statement. Press releases are

simple announcements made by the METD to inform citizens and the media

communication, of activities that were planned or in progress. Tie-

have a dissemination and publicity value, in no case can they be considered, with a

value so singular as to affirm that “they raise transparency to its maximum expression”.

sion“, since there are other more effective instruments to fulfill this function, foreseen

by the regulations and described in Law 19/2013, of December 9, on transparency,

access to public information and good governance.

Nor is it possible to infer from these that, from the beginning, SEDIA acted as a response

responsible for the treatment, since the fact of informing the public about certain

ned matters that fall within the scope of the department's competence, not

necessarily implies that the one who informs is the one who determines all the contents

about which it is reported.

The Press Releases cannot be used to assign the roles of Data Controller.

or Data Processor, since they are mere informative documents and

not attributive of competencies, therefore, it is impossible to draw this type of conclusion.

Nor is it possible to assign SEDIA the role of data controller only

because in a document on the FAQ RADAR COVID the purposes of the

treatment, nor because the SGAD is identified as the owner of the application in the

Conditions of Use of the application.

SEDIA, through the SGAD, has developed these and other applications, and has developed

carried out a dissemination task that the MSND was probably not in a position to

to do because the pandemic situation required greater dedication to other issues.

most relevant in the field of its competences.

With regard to citizens, and as has been pointed out, it was the Government that promoted

the creation of this application and urged the population to use RADAR COVID, since

it was an application that could help mitigate the pandemic at a time of boom

of infections and, furthermore, it was a solution that was being put into operation

development in practically all the countries in our European environment, so there is no

it can be affirmed that it was SEDIA that, due to press advertisements, had an appearance

experience for citizens as data controllers when their role was simply

fully contribute, in collaboration with the entire Government, to provide solutions in the

scope of its powers to promote the digitization of administrations

(and all this without taking into account that the very existence of legal categories

cases such as those responsible for and in charge of data protection processing are

hardly apprehensible for the common recipients of an informative note

ministerial, not even for non-specialized legal operators, and claim that the

general population can draw the conclusions and the subsequent attribution of roles

posed by the motion for a resolution reading a press release and bringing annu-

given some breaches of current regulations exceeds, in our opinion, what is reasonable.

noble).

And as has already been pointed out, the fact of collaborating, promoting and having a relevant role

in trying to convince the population of the use of RADAR COVID, to prevent con-

infections and reduce hospital admissions and thus deaths, offering an explanation

cation of the features of the application in the media, you cannot

to lead to the conclusion that another role different from the one assigned

in the documents repeatedly mentioned. This participation can only be understood

tion from the point of view of a coordinated action of the Government in which all

the departments contributed, in a State of alarm declared to limit the consequences

stories of the pandemic.

It should be remembered, at this point, that it was not until August 6, 2020, when

published the modification of the structure of the MSND with the creation of the SGSDII, with the

consequent attribution of new competences in terms of digitization of the

health and development of Apps in health matters to this department

The AEPD also points out that this role was played by SEDIA without legal coverage.

gal to carry out this role and without delegation or entrustment that allows the exercise

of competition, an issue that cannot be admitted as the SE-

DIA exercise another role other than that of treatment manager, which was the one assigned to

fallen.

B.3 Regarding the role of INDRA

SEDIA, in its capacity as treatment manager, counted from the first mo-

ment, with the authorization of the MSND, as data controller, for the con-

treatment of INDRA, which had sufficient guarantees to guarantee the application

cation of the GDPR.

B.4 Regarding Impact Assessments

The AEPD points out on page 184 that: "the CEPD considers that it must be carried out

a data protection impact assessment (DPIA) before starting

to use an application of this type because it is considered that the treatment can

of entailing a high risk […]. The CEPD strongly recommends the publication

tion of DPIDs.”

First of all, it is worth mentioning that although the EIPD published in September 2020 was version 1.1, a version 1.0 of the EIPD already existed prior to August 19, 2020. The EIPD provided to the AEPD was version 1.1, since it is the one that was published, with the deployment in September 2020 of a version of the application, with support bearing of co-official languages.

During the period from August 19 to publication in September 2020, it was discussed internally on the convenience or not of its publication.

In fact, in accordance with article 3.4 of Law 40/2015, of October 1, on Regime Legal Men of the Public Sector (LRJSP), the AGE, which acts to comply with its purposes with unique legal personality, holds the status of responsible and en-charged with treatment through different bodies and has not been publishing the EIPD, nor the Risk Analysis on which they are based, of the systems it develops.

In order to comply with the CEPD's recommendation, the SGAD sought criteria from the METD Data Protection Delegate. His opinion was that, in general, these documents should not be published.

In any case, the recommendation of the CEPD was finally followed, and proceeded to publish Download the DPIA and the previous Risk Analysis in September 2020 (https://github.com/radarcovid/radar-coviddocumentation).

On the other hand, it is the criterion of the AEPD, and this is stated on page 189 of its proposal of resolution, that:

“Finally, we will indicate that the subsequent completion of the EIPD does not “correct” the lack of carrying it out at the right time and with the participation of all the stakeholders. necessary factors, especially since the lack of risk assessment and adoption of the appropriate technical and organizational measures, has already caused damage intangible in the rights and freedoms of citizens, more reprehensible if it is

of Public Administrations”.

It is worth remembering at this point that the pilot application of RADAR COVID used

simulated data, so although the EIPD was done at a time after the start of the

operation of the pilot, yes it was done prior to the moment in which the appli-

cation was going to handle user health data.

B.5 Regarding the conditions of use and privacy policy

The AEPD indicates in its proposed resolution (p. 174) that: “Of the proven facts

two, it is accredited that the first version of the App planned for the program pi-

lotto (July 2020), collected in two different documents the information related to the privacy

city:

* Terms of use: https://radarcovid.covid19.gob.es/terms-of-service/use-

terms.html

* Privacy Policy: https://radarcovid.covid19.gob.es/terms-of-service/pri-

emptypolicy.html. However, none of them defined who was responsible.

ble or in charge of the treatment.”

It should be remembered that the first version of the App (pilot) was used for testing purposes.

bar aspects such as usability, perception of privacy, and effectiveness of the solution in

a simulated environment. In no case were the health data of the participants handled.

you in the pilot.

And the Privacy Policy of the app included the following notice:

“The USER of this application is warned that when downloading the application

tion on your mobile device and using it, you are merely participating voluntarily

mind in a PILOT EXPERIENCE WITH FICTITIOUS DATA alert of

COVID-19 infections on THE ISLAND OF LA GOMERA.

It is also reported that this application will stop working once

complete the pilot experience.

Therefore, in the use of the application, all notifications of exposures to

possible contagion of the disease that the user may receive correspond to

simulated assumptions and, for the same reason, as it is a pilot experience,

lotto with fictitious data, suggestions for adopting preventive measures and

care providers who, after this notification, provide the application have no other value.

need to check that the application is capable of providing suggestions of that

type to a user who received a notification of exposure to possible contact

gio".

The RADAR COVID team has been reviewing and updating the documents with the

encouragement to improve its content and facilitate its reading and understanding, making use of its

faculty of proactive responsibility in the constant improvement of the app and its documentation

associated tation.

Additionally, additional issues have been incorporated such as interoperability

through the European Interoperability Node for National Applications

contact tracing (European Forwarding Gateway Service -EFGS). Must

indicate that for the connection of RADAR COVID to the European interoperability node

system information, conditions of use and privacy policy of the

application, and was approved by the Joint Group of Data Controllers

(eHealth Network Joint Controller Group), where the MSND of the Government of Spain fi-

was listed as one of the members.

With each update of the application (following the principle of proactive responsibility)

va), if there was a change in the conditions of use and privacy policy, it was requested

again express consent by users.

On page 175 of the proposal, the AEPD states: “It is not clear who is the res-

responsible for the treatment nor the data of the Data Protection Delegate,

that are not even mentioned in the privacy policy.”

It should be remembered by SEDIA that the current privacy policy (https://radarco-

vid.gob.es/politica-de-privacidad) establishes as data controllers the

Ministry of Health and Autonomous Communities, and as the person in charge of treating

ment to the General Secretariat of Digital Administration.

On page 178 of the sanctioning resolution proposal, the Agency states: “In

sum, the privacy policy has been modified in numerous aspects until

such a point that it supposes an increase of 700 words to the initial version” .

The increase corresponds to more extensive explanations of the privacy sections.

ity, as well as the extension to new uses of the application, such as interoperability

with the contact tracing applications of the European Union.

On the other hand, any changes to the application including new functionalities

(such as the connection of RADAR COVID to the European Interoperability Node) has led to

ved the update of the conditions of use and privacy policy, in order to provide

provide transparency and information to the users of the application.

On page 179, the Agency states: “In short, SEDIA, acting as the party responsible

treatment, did not take the appropriate measures to provide the interested party with all the information

training in the terms established in articles 12 and 13 of the RGPD. This information

information, it should have been provided in a concise, transparent, intelligible and easily accessible way.

process, 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 App make it difficult

for citizens to know and understand if they are being collected, by whom and for what purpose.

purpose, personal data that concerns him, as in the case analyzed."

SEDIA wishes to remind in this regard that the conditions of use and privacy policy

emptiness have always been accessible to those interested, both from the application

mobile, such as from the web http://radarcovid.gob.es.

Therefore, the express consent of the user is necessary to be able to use the

application, besides being its totally voluntary use.

In the time that the application has been operational, SEDIA has not received any que-

either formal or informal, of the MSND Data Protection Delegate in relation to

tion to the RADAR COVID application.

On p. 181 of the proposal concludes: "Indicate that initially it was not included

information regarding the person in charge, recipients or the rights of articles 15 to

22. The final version has not included the information regarding the Delegate of

Data Protection……..".

From SEDIA, just remember that in the section "How is my privacy protected?",

the app collects the following:

“Here is a list of some of the measures with which RADAR CO-

VID 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 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 its user”

Regarding the vulnerabilities detected

B.6

As already indicated on previous occasions by the SGAD, the vulnerability re-

ported by a group of privacy experts was known in mid-Sep-

tember 2020. It was analyzed and a correction was scheduled to coincide with a

next app release. It was corrected on October 8, 2020, and shared

do the code that corrected the problem with the technical team of the Polytechnic School

Federal Government of Lausanne (EPFL), which is the one that had promoted the DP3-T protocol, guaranteed

you of privacy.

The correction was addressed within reasonable timeframes according to its impact.

As was argued to the AEPD, the scenario in which it could ex-

plotting the vulnerability, with a third party with sufficient capacity to spy on networks

of communications, and to cross the information sent by RADAR COVID with other

information at their disposal, which would allow establishing a relationship between the identity

of the user and his positive medical condition for COVID-19, was very remote.

This judgment proved correct, since it has not been detected nor is there evidence that

this theoretical vulnerability has been exploited or taken advantage of in any real case,

probably because of the difficulty and little benefit that would be obtained from its implementation.

It is known by all that there is no computer system that is 100% secure, and

Once these circumstances were considered, it was decided to continue the development (applying

using the principle “in dubio pro actione”). Since the alternative was to stop the use and

development of the app with the consequent risk and detriment to collective health, by

deprive society of a tool with a great potential to help in its full state.

health emergency alarm.

III. CONCLUSION OF THE ARGUMENTS BRIEF

SEDIA is aware that there may be discrepancies in the criteria on the actions
situations in which the start-up work has been completed, in a time
reasonable, of a necessary application in the context of a pandemic in which
rolled, with a declared state of emergency. But he has always acted with a res-
proactive responsibility to correct possible errors or omissions of the App, assuming
protecting the principle of privacy by design, acting in defense of the public interest
public and citizens, and collaborating with the AEPD in everything requested.
In fact, SEDIA requested a report from the AEPD at the time it was scheduled
the extension of the application to the Autonomous Communities in August 2020, at which time
The contribution of the AEPD would have been very valuable, but the beginning of the preliminary actions
vias, determined in the opinion of the AEPD the impossibility of having this report.
As we have already pointed out before and now repeat, the emergency situation and the
statement the state of alarm altered the ordinary legal order and the way of acting
usual administration.
The exceptional situation determined a modulation in the administrative procedures
administration and demanded to act quickly in order to be able to arrive on time and that the application
tion fulfilled its goals at a time when all the governments of our
European and international environment, they were demanding it. And we had to develop
pilot application with simulated data, emergency hiring had to be done
in which essential procedures were suppressed, in favor of agility, and it was necessary to extend
rapid application to the Autonomous Communities through the most immediate legal instruments.
diates and in accordance with the situation that would allow the legal coverage and the
streamlining of bureaucratic procedures.
The pertinent evaluations were made, the analyzes that allowed the haste with which
the application had to be developed and it was always acted with the ultimate goal of exercising
develop a proactive responsibility to allow adequate respect for the protection

of personal data.

In short, according to the previous arguments and reasoning, SEDIA

considers that there is no place for a warning sanction, because there has been no

flagrant, conscious and deliberate compliance with data protection regulations

and of all the articles that are cited in the proposed resolution of the sanction file.

tioner.

IV. SUPPLEMENTARY CONSIDERATIONS

By means of an independent document, SEDIA has requested, by virtue of what is established in

article 89.2 of the LPACAP, the practice of the test consisting of making available

position of the SGAD of the following documentation that is considered fundamental

for the exercise of the defense in the sanctioning procedure opened in relation to the

RADAR COVID app:

a) Proposed resolution of the Instructor in relation to the procedure

opened against the MSND by the RADAR COVID application, in order to appreciate the

criteria of the AEPD in relation to the activity carried out by said department.

ment that although it enjoys the same legal personality as SEDIA, it is

treated by the AEPD as a different entity.

b) Full reports of the Legal Office of the AEPD cited that are cited in

the Ninth Legal Basis (17/2020 and 32/2020) of the Proposal for

Resolution, to be able to appreciate it as a whole and accept or refute it according to

be your discretion.

(Italics, bold, and underlining are from SEDIA).

These allegations will be answered in the FD of this Resolution.

Of the actions carried out in this procedure and the documentation

in the file, the following have been accredited:

PROVEN FACTS

FIRST: Royal Decree 403/2020, of February 25, develops the organizational structure

basic information of the Ministry of Economic Affairs and Digital Transformation. Was published

on February 27, 2020 in the BOE, entering into force on the same day of its publication.

It provides in its article 1 that the METD is responsible for

“Telecommunications policy 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

“the promotion of the digitization of the public sector and the coordination and cooperation

interministerial relationship and with other Public Administrations regarding said

matters, without prejudice to the powers attributed to other departments

ministerial”.

The SGAD, according to article 9, is:

“The governing body to which it corresponds, under the authority of the person in charge

of the Secretary of State for Digitization and Artificial Intelligence, the direction,

coordination and execution of the powers attributed to the Department in

matter of digital transformation of the administration, including the development and application of Laws 39/2015, of October 1, of the Procedure Common Administrative Law of Public Administrations, and 40/2015, of 1 October, and its regulations, regarding the performance and func- operation of the public sector by electronic means."

SECOND: Royal Decree 454/2020, of March 10, which develops the 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.

In its article 1 it provides:

It corresponds to the Ministry of Health, the proposal and execution of the policy of the Government in matters of health, planning and healthcare, as well as as the exercise of the powers of the General State Administration to ensure citizens the right to health protection.

In its article 3 it 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; (...).

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. (…)".

THIRD: Royal Decree 463/2020, of March 14, which declares the state

of alarm for the management of the health crisis situation caused by the COVID-

19, in article 4.2.d) designates the Minister of Health as the competent authority de-

legacy in your area of responsibility.

FOURTH: 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.

FIFTH: 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

DDD

E.E.E.

F.F.F.

GGG

H.H.H.

I.I.I.

J.J.J.

L.L.L.

HMM.

N.N.N.

Ñ.Ñ.Ñ.

O.O.O.

PPP

Q.Q.Q

The issues discussed are:

SEDIA / CCAA / Ministry of Health / Minsait

SEDIA

SEDIA

SEDIA

SEDIA

Ministry of Health

Ministry of Health

SEDIA

Canary Islands Government

Minsait

Minsait

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.

SIXTH: 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, Nadia Calviño, together with the Secretaries of State of Digital

ization and Artificial Intelligence, Carmen Artigas., and Telecommunications and Infra-

Digital Structures, Roberto Sánchez, participated in this meeting to seek

establish a common European position that allows taking advantage of the possibilities that

offers the technology to contribute to the management of the pandemic and the subsequent re-

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. (…)

The Secretary of State for Digitization and Artificial Intelligence, Carmen Artigas,

shared with the autonomies the position of Spain at European level, as well as

advances prepared by the European Commission on these digital tools.

The aim is to join efforts and share points of view on the possibilities

existing around the development of these applications and their interoperability,

ing coordinated responses based on the needs of the different territories.

rivers".

SEVENTH: On June 9, 2020, the General Director of Public Health, Cali-

and Innovation of the MSND sent a letter to the Secretary General of Administration

Digital (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."

EIGHTH: On June 11, 2020, the already repealed Royal Decree enters 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.

NINTH: On June 15, 2020, it was agreed by the Secretary General of the

Digital Administration contracting services for contact traceability

in relation to the pandemic caused by COVID 19 to Indra Tecnologías de la In-

formation S.L.

As stated in the "Condition specifications for the design, development, pilot and evaluation

tion of a system that allows contact tracing in relation to the pandemic

caused by COVID-19" dated June 10 and 12, 2020, section 1 under the

"Background" heading:

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 Development of

technological solutions and mobile applications for data collection

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.

As stated in the object of the contract, the implementation project would have three phases:

pre-pilot phase, pilot phase and post-pilot phase.

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

that allows contact tracing in relation to the pandemic caused by the co-

vid-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 necessary that the Backend developments be carried out in an infrastructure

in the cloud in self-management mode, to facilitate agility in the development of

the solution.

Notwithstanding the foregoing, both the storage and any activity of

data processing will be located in the territory of the European Union, whether

These are provided and managed by the successful bidder or by its contractors.

and collaborators, and will be hosted on servers and/or data processing centers

of the successful bidder itself or of its contractors.

…

As far as possible, the use of components in the in-

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

SARA of the AGE.

6.1. General Confidentiality

The contractor undertakes to guarantee the strictest confidentiality and re-

reserves over any data or information to which it may have access or

made known on the occasion of the execution of the contract, as well as on the requirements

results obtained from their treatment, and that they will only be used for the

achievement of the object of the contract, not being able to communicate, use, or

transfer them to third parties under any circumstances, not even for their conservation. It is-

These obligations extend to all persons who, under the dependency

of the contractor or on their behalf, have been able to intervene in any of the

contract execution sessions.

The obligation of confidentiality and reserve entails that of custody and prevent the

access to the information and documentation provided and to those resulting from their

treatment of any third party outside the contracted service, understanding

as such, both any person outside the contractor company and any other

ra that, even if not, 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 that resulting from its processing.

protection against unauthorized modification or destruction of data.

6.2. Personal data protection

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

Protection of Personal Data and guarantee of digital rights, adapted

ted to Regulation (EU) 2016/679 of the European Parliament and of the Council,

April 27, 2016, and by which Directive 95/46/CE (Regulation

General Data Protection), including the provisions of the additional provision

first of the Organic Law 3/2018, of December 5 and in the Royal De-

decree 3/2010, of January 8.

In accordance with the first additional provision of Organic Law 3/2018, of 5

December, on Security measures in the public sector, the me-

security measures to be applied within the framework of personal data processing

will correspond to those of the original public administration and will be adjusted

will be assigned to the National Security Scheme.

INDRA INFORMATION TECHNOLOGY SOLUTIONS will be required to

SLU the express manifestation of submission to national regulations and the

European Union in terms of data protection in accordance with the articles

35.1d and 122.2 of the LCSP modified by article 5 of the Royal Decree Law

14/2019, of October 31, by which urgent measures are adopted for reasons

public security measures in matters of digital administration, contracting of

public sector and telecommunications.

6.3. Security

INDRA SOLUTIONS TECHNOLOGIES OF INFORMATION, SLU implemented

will promote the appropriate technical and organizational security measures and develop

The pertinent documentation will be prepared, in accordance with the corresponding analysis

of risks, as established in Royal Decree 3/2010, of January 8, by

which regulates the National Security Scheme in the field of Administration

electronic nistration.

7 INTELLECTUAL PROPERTY

Without prejudice to the provisions of current legislation on property

intellectual property, the successful bidder expressly accepts that the ownership of all

products that are made by the successful bidder, including its employees and

where appropriate, any subcontracted company, in execution of the Contract and, in

particular, all the intellectual and/or industrial property rights deriving

come from them, corresponds only to the contracting administration,

exclusively and with no limitations other than those imposed by the

legal system.

For the purposes set forth in the preceding paragraph, the successful bidder is comprised of

promises to deliver to the SGAD all the technical documentation, works and

materials generated, in whose possession they will remain at the end of the Contract

without the contractor being able to keep it, or obtain a copy of it, or use it or

provide it to third parties without the express authorization of the SGAD, which would give it, in its

case, prior formal request of the contractor with an expression of the purpose.”

It also includes in ANNEX I the characteristics of the mobile application system and the

backend element in public infrastructure:

ANNEX I. CHARACTERISTICS OF THE MOBILE APPLICATION SYSTEM

1. Start and welcome application: legal notice, informative onboarding, activation

Bluetooth tracking. Use of anonymous Google/Apple SDK and redirection to

generic repository (Backend).

a. Allows the user to transmit and receive random identifiers.

tory via Bluetooth

b. Verification of the authorization code by the health authority

taria before positive for COVID-19. Facing the pilot, as expected

that the service of the health authority is not available, the

validation of the positive that triggers the tracing process and can be

gives to pilot

c. It sends its ephemeral key generator beacon to the server in case of

positive.

d. Informative static screens.

and. Interaction with the google/apple SDK, according to functionality

provided:

Yo. Manage daily random keys:

1. Generate daily temporary exposure keys

them and rotate ephemeral identifiers based on them.

2. Provide the keys to the Backend for diagnostic users

including temporary values.

3. Accept the keys of the App for exposure detection.

tion, including dates and risk levels of

transmission.

4. Store keys on the device.

ii. Manage Bluetooth sending and scanning:

1. Management of sending keys.

2. Scan keys issued by other devices.

3. Store the observed keys in a storage

I lie on the device.

4. Identify when another user in contact has been a

confirmed case.

5. Calculate and provide the risk of exposure to the application

tion.

6. Submit the following permission requests to the user

river:

a. Before you start scanning and sending the keys

you see.

b. Before providing the server with the keys to the server,

central pain after being infected.

2. Communication of positive cases:

a. Enter QR/COVID-19 code (manual, scanner or import)

personal and single use.

b. Confirmation notice QR validated positive: informative screen.

c. Optional questionnaire (if positive): collects anonymous data

basics for your treatment Backend App (zip code, symptomatology

and its date, previous pathologies,…).

3. Risk notification: contact notification with confirmed positive and screen

of recommendations.

4. Application exit: possibility of exiting the application at any

time, removing any trace of ephemeral keys used.

BACKEND ELEMENT IN PUBLIC INFRASTRUCTURE

1. Backend data management

a. Serve information necessary for the operation of the App (if it is

time necessary. Alternatively the App can be self-contained).

b. Validation with the health authorization system before diagnoses

positive (if this system were not available, a Si-

simulation of this validation). The application must communicate with a

external server (sanitary) that provides the authorization code that

confirm the positive and can authorize uploading the beacons to the service in

function of the following proposed cycle:

Yo. Medical system requests token/QR authentication to the Backend

to confirm positive COVID-19.

ii. Patient receives token/QR authentication to confirm possi-

tive COVID-19.

iii. Patient sends the authorized token/QR to the Backend to upload

your contact history.

As it is foreseeable that the service of the authority is not available

In the initial scope, the validation of the positive will be simulated

trigger the tracing process so that its functionality can be tested.

birth.

c. Database with centralized information service that allows the tracking

contact trao and beacon management.

Yo. Collect beacons from users who have been diagnosed

of COVID-19.

ii. Distribute beacons of confirmed cases to devices.

iii. Positive authorization service integration.

IV. Integration with Third Party systems. Interoperability study

with Backends from other States to ensure cross-border functionality

dull

2. Security

a. Implementation of controls to prevent specific attacks at the

of application.

b. Securing communications with other devices and systems

sanitary.

c. Anonymization of signals between devices.

3. Simulation: ability to emulate positive COVID-19 response, for purposes of

testing (test tracing behavior).

TENTH: SEDIA has accredited the following certificates issued in favor of IN-

DRA:

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

information that support business processes and information assets

necessary for the provision of IT outsourcing services Admin-

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

physical and virtualized cloud), according to the statement of applicability

in force on the date of issuance of the certificate.

o ISO 27001 Information Security Management System Certificate.

mation: The information systems that support the processes of ne-

business and information assets necessary for the provision of services

IT outsourcing services Administration, Support, Exploitation and Infra-

structure), both in physical and virtualized cloud environments), according to

the declaration of applicability in force at the date of the audit.

journalism

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

Information technologies: The SMS of IT outsourcing services

Administration, Support, Exploitation and Infrastructure), both in environments

us physical and virtualized cloud), according to the catalog of services in

vigor. Certificate of the Technology Service Management System of

Information. For the management of the RADAR COVID system, INDRA has

contracted the services of Amazon Web Services INC.

ELEVEN: On June 17, 2020, a meeting of the working group is held.

low interterritorial attended by representatives of the Autonomous Communities of

Andalusia, Aragon, Asturias, Castilla y León, Extremadura, Galicia, Balearic Islands, Is-

the Canary Islands, La Rioja, Madrid, Murcia, Navarra and Valencia and the autonomous city of

Melilla, as well as by the Secretary of State for Digitization and Intelligence

Artificial attend G.G.G., Deputy Director General for the Promotion of Digitization of the Ad-

administration, F.F.F., technical advisor for the development of the application, the technical team

co in charge of application development and R.R.R., Cabinet advisor.

It is stated that:

"…three main objectives of the application: preserve public health, go a

stay ahead of COVID-19 and minimize its economic impact by facilitating

the movement of people. To do this, there are three key moments to keep in mind:

account: the activation of Bluetooth (which allows to preserve the anonymity of the

users), the report of positive diagnoses and the notification to users in

risk of contagion.

(…)

The importance of privacy for the application is also highlighted, guaranteeing

maintaining the anonymity of people at all times, allowing the

app can be deactivated at any time, storing the data for-

decentralized ma only for 14 days or generating the notices in the own

app.

Finally, it explains how the application behaves technically: the telephones

random Bluetooth identifiers are exchanged with us and, with the consent

of the user, the phone loads the history of the last 14 days of keys in the

server. Each phone periodically downloads Bluetooth keys from all

diagnosed people who have reported it and who may have been in

Contact. With this, the contagion alert notifications are sent."

TWELFTH: There is a document called "Covid-19 App Pilot Design. Pre-

CCAA statement June 17, 2020, prepared by SEDIA.

This defines the key parameters of the Pilot:

a) Duration

• 15 days of active APP

• Tentative start date: Week of June 29.

b) Location:

• San Sebastián de La Gomera (7,921 inhabitants, INE provisional data

01/01/2020), municipality located on the Island of La Gomera.

c) Participants:

• Residents in the municipality captured by different access channels to the pi-

lotus.

• Tourists residing in Tenerife who simulate movement through the municipality

during the pilot.

d) Pilot Scope: Volume of participants

• The greatest possible participation will be promoted by combining different channels

of access to it, estimating a volume between 2,000 and 3,000 users.

rivers of the APP.

• Approximately 10% of cases will be established with COVID Positive

initial simulated, to favor the detection of cases of risk and thus com-

test APP operation.

e) Assessment of compliance with objectives

• Quantitative data analysis

• Qualitative analysis: anonymous surveys and remote user tests (15

users).

It also collects the "Pilot Access Channels" by the participants:

4 access channels to the APP are proposed for controlled participation in the

pilot, to be confirmed with the government of the Canary Islands and the local government of La Gomera

1. Individual direct communication to Public Employees

People who reside in San Sebastián de la Gomera and work as

public employees in different areas and people residing in Tenerife and

can travel as "simulated tourists" to the municipality during the pilot

2. Installing Agents

Team of agents that will promote and help in the download of the APP in

public spaces and citizen service offices in the municipality, enhancing

capturing young people and people over 65 years of age

3. Specific information telephone

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

87/212

Possibility of enabling a telephone to facilitate access to those

citizens of the municipality who are interested in participating, as well as to

possible simulated contagion check

4. Postal mailing

Evaluate the possibility of direct letters or brochures deposited in a physical mailbox

all residents in the municipality to explain the pilot and invite them to participate

THIRTEENTH: There is, dated June 23, 2020, a press release published

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 objective of the pilot is to evaluate technical aspects and user experience

of the citizen, in order to optimize the design of the application and its degree of

bail. It will also serve to calibrate the app's algorithm in order to guarantee

the veracity of the notifications. (…)

Once the pilot test has been completed and evaluated in a real scenario, all

make the appropriate decisions for the connection with the health system of the different

different autonomous communities.

This technological tool is added to the measures already implemented by

health authorities to follow the contacts of COVID-19 infections

and that, together with the preventive measures adopted, are contributing to the con-

pandemic troll. The contract approved by the Council of Ministers by the procedure

emergency assistance has been signed with the company Indra Soluciones Tecnológi-

Cases of Information S.L.U. for an amount of 330,537.52 euros, VAT included.

(…)

Privacy

The development uses a decentralized model, based on the Decentralized protocol.

zed Privacy-Preserving Proximity Tracing (DP-3T), the most respectful of privacy

user city. This implies that only the identifiers are sent to the server.

encrypted that each mobile emits, not those received from other nearby terminals.

From time to time, mobile phones download new contagion identifiers

confirmed to compare with your records. That is, the comparison of data and

risk analysis is always carried out on the user's mobile phone and not on a service.

dor, which guarantees privacy.

This application complies, therefore, with all the guarantees established by the regulations

to safeguard the privacy of citizens. In addition, it guarantees the

proportionality and minimizes the use of personal data. The use of the application will be voluntary and framed within the limits of the health emergency, strictly compliance with the recommendations of the European Commission in this regard."

FOURTEENTH: It is recorded, dated June 23, 2020, in the Reference of the Con-Council of 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 BY 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."

FIFTEENTH: On June 29, 2020, it is launched by the Government of Spain

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 (https://radar-resources.s3-eu-west-

1.amazonaws.com/28-01-2020-InformeRadarCOVID.pdf) 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

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

90/212

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:

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-

due to 3 key factors

leave it open

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, aggregated information has been collected from the users of the application.

cation, both of the people who downloaded it, and of the people

who assumed the role of Positive Cases or received alert notifications of

risk of contagion.

This aggregate information prevents obtaining behavioral information or by

more qualified profiles of citizens, as well as a sociological analysis of

spread of the virus.

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 analysis of (sic)

actual spread of the disease that would be monitored by the app.

Methodology.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

92/212

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

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 con-

servants 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 in-

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.

SIXTEENTH: There is a document called “COVID Radar. Secretary General

General of Digital Administration. General operation. Madrid, June 2020” where the

SEDIA reports the following:

Covid-19 app strategy

Objectives of the app

• Preserve public health without giving up the privacy of citizens

• Be one step ahead of Covid-19: alerting people at risk is containing

the virus proactively

• Minimize the economic impact of Covid-19, by controlling the pandemic without

drastic measures and facilitating the movement of people

the key moments

• Bluetooth activation

• Report of positive diagnoses

• Notification to users at risk of contagion

Focus on privacy

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 first version of 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 positive COVID-19 is diagnosed or when the Medical Service

consider necessary

• 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

It also contains the "Functional description of the app" and the "Operation of the alerts".

Bluetooth contagion rates".

SEVENTEENTH: There is a document called "Radar COVID. Tracing:

07.17.2020", prepared by SEDIA together with the Canary Islands Health Service, the Government

of the Canary Islands, the Government of the Cabildo of La Gomera and the City Council of San Sebas-

tián de La Gomera where the following is reported:

What do we observe daily?

Citizen behavior

Radar COVID Accumulated Downloads: 54,591

• There are more than 54,000 downloads nationwide, 94% on Android

• Of the almost 10,000 downloads since the beginning of the pilot, our pro-

engines have confirmed 924 downloads, plus 59 on the web

• Unloading has been promoted among 758 volunteers or public employees.

cos

And regarding the Action Plan Phase 3- Week 20 to 27 July

Analyzing data and drawing conclusions, says:

C/ Jorge Juan, 6

28001 – Madrid

EIGHTEENTH

: On July 21, 2020, a meeting is held that has

Its purpose is the “Design, development, pilot and evaluation of a system that allows the tra-

reliability of contacts in relation to the pandemic caused by Covid-19”.

Attend:

Person

DDD

E.E.E.

F.F.F.

GGG

S.S.S.

TTT

H.H.H.

I.I.I.

L.L.L.

HMM.

N.N.N.

Ñ.Ñ.Ñ.

O.O.O.

Q.Q.Q

SEDIA / CCAA / Ministry of Health / Minsait

SEDIA

SEDIA

SEDIA

SEDIA

Canary Islands Government

SEDIA

Ministry of Health

Ministry of Health

Canary Islands Government

Minsait

Minsait

Minsait

Minsait

Minsait

Issues discussed:

The attached document is presented 20200717_SEDIA Monitoring v13.PPTX

where the advances in the COVID Radar pilot are collected.

Agreements adopted:

It is agreed to present a complete report to the next monitoring committee.

with the analysis of the conclusions that have been drawn from the execution already

end of the pilot on the island of La Gomera.

NINETEENTH: 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 compiling proposals from the Autonomous Communities, we opted

by a centralized code generation scheme and decentralized management

zada

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

Pilot results. What conclusions do we draw about the success of the pi-

lotus?

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 is effective detecting close contacts since its recalibration

on July 15*, by being able to detect contacts of people close to the user

and strangers

Regarding the "Simulation of the COVID Radar Application outbreak: final data"

reports:

What useful recommendations or lessons can we extract in the face of a study?

national draft?

Analysis:

•

Instrumentation for anonymous data collection to analyze the de-

Radar COVID performance more accurately than anonymity

current total facilitates.

• Calibrated: track aggregate statistics and calls to the call center

for calibration of Bluetooth weights in order to avoid generating so-

brealert without giving up a useful volume of contact notifications is-

generated stretch.

TWENTIETH: On July 27, 2020, a meeting is held with the purpose of

the "Design, development, pilot and evaluation of a system that allows the traceability of

contacts in relation to the pandemic caused by Covid-19".

They include as attendees:

Person

DDD

E.E.E.

F.F.F.

GGG

H.H.H.

I.I.I.

J.J.J.

L.L.L.

HMM.

SEDIA / CCAA / Ministry of Health / Minsait

SEDIA

SEDIA

SEDIA

SEDIA

Ministry of Health

Ministry of Health

SEDIA

Canary Islands Government

Minsait

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

99/212

Person

N.N.N.

Ñ.Ñ.Ñ.

O.O.O.

PPP

Q.Q.Q

Issues discussed:

SEDIA / CCAA / Ministry of Health / Minsait

Minsait

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.

Agreements adopted:

It is agreed to have the list of ac-

tions to be carried out on the app with a view to its imminent production

you, either in a CCAA, city or at the national level. It is also remembered to prepare

Create a descriptive document with a summary of how the app works

so that the different CCAA can analyze its operation.

TWENTY-FIRST: There is a document called “Radar COVID. Follow-up

project document 07.31.2020”, where SEDIA defines the launch activities re-

recommended for the roll out:

TWENTIETH

SECOND

press:

: On August 3, 2020, the METD publishes this note of

“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, Carmen Artigas, at a press conference in which she shared the results

ted obtained during the pilot. Along with it, A.A.C., di-

General Director of Public Health and Innovation of the Ministry of Health, A.A.D.,

General Director of Modernization and Quality of Services of the Government of Ca-

narias, G.G.G., deputy director general of the Promotion of Digitalization of the Administration

tration, and F.F.F., technical advisor to the 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, a meeting is held to

Its purpose is the "Design, development, pilot and evaluation of a system that allows the

traceability of contacts in relation to the pandemic caused by Covid-19".

They include as attendees:

Person

DDD

Ms. F.F.F.

GGG

V.V.V.

I.I.I.

W.W.W.

X.X.X.

HMM.

SEDIA / CCAA / Ministry of Health / Minsait

SEDIA

SEDIA

SEDIA

SEDIA

Ministry of Health

CCAES

CCAES

Minsait

C/ Jorge Juan, 6

28001 – Madrid

Person

N.N.N.

Ñ.Ñ.Ñ.

O.O.O.

Y.Y.Y.

Q.Q.Q

SEDIA / CCAA / Ministry of Health / Minsait

Minsait

Minsait

Minsait

Minsait

Minsait

Agreements adopted:

It is agreed to have the app ready by Monday 08/10/2020 introducing the changes

discussed in the attached documents facilitating an emergency exit in the short

deadline to those Autonomous Communities that request it and continue advancing in the development of the versions for departure nationwide.

TWENTY FOURTH: 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 FIFTH: 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 application.

cation Radar COVID (pilot version), contains the following information:

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.

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 SIXTH: In the initial version of the "Conditions 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

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

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

TWENTIETH

: On August 12, 2020, it is prepared by SEDIA, and according to

SEVENTH

ma SEDIA itself, the first EIPD document regarding the Radar pilot project

Covid, “when the decision was made to adapt the pilot project for its de-

fold at the national level”.

Said document affirms the existence of data processing of a personal nature.

sound:

“Therefore, in cases where, at first glance, the information does not allow syn-

regularize a certain person, this person can still be identifiable, because

that information can be combined with other data, whether the controller

of their treatment has knowledge of them as if not, that allow to distinguish

guide that person from others.

Although pseudonymized data was traditionally considered

anonymous data, pseudonymization is now no longer considered a

method of anonymization, since the person is still identifiable, even if it is

indirectly. Thus, it is currently considered that pseudonymized data

Both are still personal data and are subject to social regulations.

on protection of personal data.

In conclusion, in this treatment, despite the fact that users cannot be

identified directly, they could become identifiable, carrying out ma-

pas of relationships between people, through reidentification by im-

implicit, even being able to identify the identity of those infected.

It must be taken into account, in this sense, that the processing of information

not only affects the user of the application but also that of all third parties.

rivers with which he has been in contact.

Having said the above, starting from the fact that the treatment activity

The processing in question applies the current regulations on privacy and protection

of data, and taking into account the category of data that could come to identify

tify the users, the need to carry out an EIPD is analyzed".

Regarding the roles of "Responsible, co-responsible and in charge of the treatment

to" has:

"Therefore, and by virtue of the provisions of article 27.3, those responsible for the

treatment will be the autonomous communities, the cities of Ceuta and Melilla

and the Ministry of Health, within the scope of their respective powers, which

will guarantee the application of the mandatory security measures that result
of the corresponding risk analysis, taking into account that the treat-
treatments affect special categories of data and that said treatments are
will be carried out by public administrations obliged to comply with the
National Security burning.

In this case, the owner of the application is the General Secretariat of Administration.
Digital tion dependent on the Ministry of Economic Affairs and Transformation
ción Digital, which is also constituted as Data Controller.

The application has been developed through the Secretary of State for Digi-
Talization and Artificial Intelligence (SEDIA)".

Regarding the personal data processed, it confirms the following:

"In this way, the data generated or accessed by the application are the
following:

· The application generates proximity data (temporary exposure keys with
which the user's device has generated the random codes or IDs.
Rolling Proximity Indicator - RPI), which is data generated by the in-
Bluetooth Low Energy (BLE) handshaking between devices
within an epidemiologically relevant distance and during
for a relevant time also from the epidemiological point of view. It is-
These data will be communicated to the health authorities only when
has confirmed that a user in question is infected with COVID-19 and
condition that the person opts for this to be done, that is, voluntarily.
wishful thinking

Data through which the user is previously warned of a contact of
risk. These data allow estimating how many users are warned by the
application of a potential risk of contagion, without being able to trace your identity, and

allows the National Health Service to prepare initiatives and resources

necessary to serve the users who have received the notification.

· The day the user developed symptoms consistent with COVID-19.

· Code (QR) provided by the health authorities to allow the

user activate a warning alert. This 12-digit number will be pro-

provided by the health authorities, who will send it after giving possi-

tive. This number does not cease to be the "confirmation" that the user actually

has tested positive and it is not a random user trying to send alerts

false.

· The IP address that the device uses to connect to the Internet. In this

In this sense, it is worth mentioning the Judgment of the Supreme Court of October 3

2014, in which Legal Basis number four establishes that

«There is no doubt that, based on the IP address, it is possible to identify directly or indi-

the identity of the interested party, since the providers of access to information

ternet have a record of the names, telephone numbers and other identifying information

of the users to whom they have assigned the particular IP addresses. The

Judgment confirms that IP addresses are personal data since they contain

contain information concerning identified or identifiable persons.

(…)

Therefore, as a consequence of the above, any monitoring system

that checks a public database of diagnostic keys.

co against rolling proximity identifiers-

RPID) on a user's device leaves open the possibility that the con-

touches of an infected person find out which of the people they found

rum is infected. Furthermore, the fact that infected users share

publicly publish their diagnostic keys once a day, instead of their RPIDs

every few minutes, it exposes those people to link attacks.

Therefore, special attention must be paid to this probability, since in the

In the event that a user of the application could be identified, the privacy

would be enormously threatened, and all kinds of

personal data such as:

health data,

· Location,

· Contacts,

· Email,

call log,

· SMS and instant messaging,

· Identity of the interested party,

Phone identity (i.e. phone name)

· Browsing history,

Authentication credentials for information society services

tion (particularly services with social features)

· Photographs and videos

Biometric data (for example, facial recognition models and fingerprints

fingerprints)".

Regarding the purpose of the treatment, they determine it, linking it to the functionalities

of the application:

“Each one of the different functionalities of the application obeys certain

late swims:

· The main purpose of the App is to inform people who have been

very close to someone who happens to be a confirmed carrier of the virus, in order to

break the chains of transmission as soon as possible. In this way, the application

tion allows identifying people who have been in contact with someone

infected with COVID-19 and inform them of the measures that should be taken

afterwards, how to undergo self-quarantine or the corresponding tests.

· For this, the App maintains the contacts of the people who use the application.

tion and who may have been exposed to COVID-19 infection.

When a person tests positive for COVID-19 and decides to share li-

If this information is disclosed, the App alerts those other people who could have

been infected and with whom you have had contact in the last 14 days. For

this, this person must share a 12-digit number that will be provided

approved by the health authorities. The mobile performs a check to see if the

Random IDs match one that has been marked as positive.

· The day on which the user developed symptoms compatible with

COVID-19 and date of contact with infected persons.”

From the study of the life cycle of the data it is indicated that the capture of the data is pro-

duce with the "Access to information stored on the mobile device at the time

of the installation of the App”.

TWENTY-EIGHTH: 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-NINTH: 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 August 14, 2020, coordinated by:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

- Coordination Center for Health Alerts and Emergencies.

- General Directorate of Public Health, Quality and Innovation.

THIRTIETH: At the national level, the commissioning of the Radar COVID App was

produced on August 19, 2020.

THIRTY-FIRST: On August 26, 2020, the meeting is held to

Determine project status and next steps. The attendees are:

Person

DDD

F.F.F.

Z.Z.Z.

V.V.V.

HMM.

PPP

Q.Q.Q

SEDIA / CCAA / Ministry of Health / Minsait

SEDIA

SEDIA

SEDIA

SEDIA

Minsait

Minsait

Minsait

THIRTIETH

SECOND:

There is a first version of the document "Analysis of

Radar Service Risks Covid19” dated August 2020, prepared by

MINTSAIT an INDRA COMPANY.

THIRTY-THIRD: 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-FOURTH On September 9, 2020, the METD publishes this note

press:

“The RadarCOVID mobile application completes its implementation in thirteen communities

autonomous, 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-FIFTH: 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-SIX: There are two more versions of the Impact Assessment:

In the second 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 third 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-SEVENTH: In the final version of the "Privacy Policy of the Radar COVID Application” 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.

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).

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

125/212

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.

personal cough of users.

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

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

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-EIGHTH: In the final version of the "Terms of Use of Radar

COVID" contains the following information:

Radar COVID TERMS OF USE

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

130/212

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

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 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 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-NINTH: On October 15, 2020, the “Re-

solution of October 13, 2020, of the Undersecretariat, by which the Agreement is published between the Ministry of Economic Affairs and Digital Transformation and the Ministry of Health, about the application "Radar COVID"". Dated 10/10/2020 enters said resolution is in 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.

This indicates the competencies of the participants:

“Second.- That in accordance with the provisions of article 7.1 of the 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 National Health System (hereinafter, SGSDII) is the governing body of the Ministry of Health which, under the superior direction of the person in charge of the Department, it is up to address the modernization, innovation, improvement and transformation of the National System of Health.

Third. That, in accordance with the provisions of article 8.2.a) of the Royal Decree 735/2020, of August 4, the General Directorate of Digital Health and Information Systems Information for the National Health System is the governing body depending tooth of the General Secretariat of Digital Health to whom the design corresponds, development and implementation of the common electronic services of the System National Health, the computer applications and digital health of the Ministry of Health, as well as the sectoral and horizontal portals of said Department. ment, guaranteeing its integration and homogeneity

Fourth.- That in accordance with the provisions of Royal Decree 403/2020, of 25 February, which develops the basic organizational structure of the Ministry of

Economic Affairs and Digital Transformation, corresponds to the General Secretariat

Directorate of Digital Administration (hereinafter SGAD), the governing body of the Sec-

Secretary of State for Digitization and Artificial Intelligence, the direction, coordination

nation and execution of the powers attributed to the Secretary of State in

matter of digital transformation of the administration".

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 application

"Radar COVID" that correspond to the General Directorate of Digital Health

and Information Systems for the National Health System under the

provided for in article 8.2.a) of Royal Decree 735/2020, of August 4, by the

development of the basic organic structure of the Ministry of Health, the

General Secretariat of Digital Health, Information and Innovation of the Na-

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

tion 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

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 paragraph 1 and 2 reads:

1. In the collaboration agreements that the SGAD signs by delegation

of the Ministry of Health for the adherence of the autonomous communities and cities

Except for the use of the "Radar COVID" application, the SGAD will commit to

fulfillment of the following obligations:

a) The provision of the use of the Application in accordance with the provisions of the

Agreement.

b) The distribution to the competent ministries in matters of health of the

positive codes necessary for users of the Application with test

positive PCR enter them in it, thus guaranteeing the non-existence of

false positives in the system.

c) The adoption of the necessary security measures to protect the information

contained in the application and the systems associated with technological solutions

cas object of said Convention.

d) The assumption of the commitment not to re-identify the interested parties.

e) The assumption of the commitment not to store codes or elements

that could allow the reidentification of people, including di-

IP addresses.

f) The establishment of deadlines 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.

g) The assumption of the commitment not to carry out unilateral processing

of the data, giving rise to different treatments or treatment operations.

those established in the agreement or similar that had not been foreseen

in said agreement.

h) The assumption of the commitment not to carry out self-decision making

nuanced or other decisions that could affect the interested parties.

i) The establishment, together with the competent ministry in matters of health

of the autonomous community or city in question, the detail of who puts

end to the life cycle of the processing of personal data and terms in which

the definitive elimination of all information should be carried out, along with

the commitment of both parties not to keep data beyond the agreement of the

end of treatment life cycle.

j) Any other obligations necessary for the successful completion of the application that the SGAD can carry out in its field of competence.

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

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.

FORTIETH: On October 22, 2020, the METD publishes this note of

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, Carmen Artigas,

held a meeting this morning with representatives of the main

telephone operators in the country with the aim of establishing ways of collaborating

tion for the dissemination of the RadarCOVID contact tracing mobile application.

The meeting is part of a series of sectoral meetings with different

actors, institutions and companies to explore possible support models

for the expansion and implementation among citizens of this digital tool.”

FORTY-FIRST: The Radar COVID App 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.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

140/212

sgsdii@sanidad.gob.es

DATA PROTECTION DELEGATE 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.

FORTY-SECOND: There is no proof that SEDIA sought the advice-

training of the METD data protection delegate, when carrying out the evaluation of

impact on data protection.

FORTY-THIRD: 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

FORTY-FOURTH: 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-FIFTH: 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. 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 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

SEDIA is accused of committing several infractions for violating the

articles: 5.1.a), 5.2, 12, 13, 25, 28.3 and 28.10 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 72.1.a) and h) and 73.d), k), m) 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. (…)

m) The infraction by a person in charge of the treatment of the provisions of the Regulation-

ment (EU) 2016/679 and in this organic law, when determining the purposes and

means of treatment, in accordance with the provisions of article 28.10 of the aforementioned

regulation. (…)

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

In relation to the allegations adduced to the resolution proposal, we proceed to

respond to them according to the order set out by SEDIA:

I. BACKGROUND

Certainly, dated February 26, 2021, by virtue of the investigative powers

granted to the control authorities in article 57.1 of the RGPD, and in accordance

In accordance with the provisions of article 67 of the LOPDGDD, the SGID issued a report

of previous investigation actions and on May 21, 2021, the AEPD

agreed to initiate the disciplinary proceedings.

Regarding the beginning of the preliminary investigation actions, the Judgment of the Au-

National Science (SAN), 4988/2007, October 17, 2007, justifies the convenience of

previous investigative actions in relation to sanctioning procedures

dors stating that:

“It is that due to the seriousness and transcendence that the exercise of the

power to sanction, since the legal status of someone who is subject to a

sanctioning file, for this single circumstance, it can be found negative

severely affected, it is necessary that the decision to initiate the procedure

sanctioning party is founded and based on solid reasons that require such

initiation.

That is, with the purpose of allowing the Administration to know the facts

foreseeable offenders, the concurrent circumstances and the persons

intervening parties, it is allowed to carry out said investigative actions

prior investigation or investigation, as necessary and timely to verify

to what extent, there is a rational basis to understand the fact produced in-

fraudster, and impute it to a specific person.”

Article 67 of the LOPDGDD establishes that:

“Before the adoption of the agreement to initiate the procedure, and once the

processes the claim, if any, the Spanish Agency for the Protection of

Data may carry out preliminary investigation actions in order to achieve

a better determination of the facts and circumstances that justify the

processing of the procedure. The Spanish Data Protection Agency

will act in any case when it is necessary to investigate treatments that

involves massive traffic of personal data”.

It should be noted that article 53 of the LOPDGDD determines the "Scope of the activity research capacity":

"1. Those who develop the research activity may collect the information precise instructions for the performance of their duties, carry out inspections nes, require the exhibition or sending of the necessary documents and data, examine them in the place where they are deposited or where they are treatments are carried out, obtain a copy of them, inspect the physical equipment physical and logical and require the execution of treatments and programs or procedures Treatment management and support procedures subject to investigation. (…)"

Thus, and taking into account the above considerations, the Agency can carry out the investigations it deems appropriate regardless of whether whether or not you have filed a claim, after which you can decide to initiate an ex officio penalty procedure (article 68 of the LOPDGDD).

In relation to the allegations made by SEDIA, we must state that the AEPD in the exercise of its powers, as conferred by articles 57 and 58 of the RGPD in which its functions and powers are established respectively, requested SEDIA the information it considered appropriate to clarify the disputed facts and determine the actions carried out by SEDIA, specifically with respect to the role cided in relation to the processing of personal data through the application.

II. ALLEGATIONS.

The allegations made to the preliminary investigation actions, to the agreement of

beginning and during the test period, were answered in the proposed resolution

dated January 26, 2022.

A) Regarding the ARGUMENTS OF A GENERAL NATURE:

It refers to RADAR COVID as an additional tool and to Royal Decree 463/2020,

of March 14. It argues that, in this context, SEDIA, as the person in charge of

procedure, acted in accordance with the instructions given at all times by the MSND,

as delegated authority of the Government in matters of public health and responsible for the

treatment. Reasons that, although these indications were not reflected as required

regulations, was due to the fact that the state of alarm made it difficult to formalize the instruments

usual procedures provided for in the legislation for these cases in circumstances

normal. It refers to the meetings held which were attended by representatives of the

MSND, SEDIA and the company awarded the emergency contract, in the

that the necessary decisions were made to advance in the development of the pilot and

the application.

In this sense, from the taking of the evidence and in relation to the meetings held

and that appear in the proven facts, the existence of any

indication “instruction” by the MSND that covers the actions carried out

rolled by SEDIA. Nor in the referenced letter of June 9, 2020, giving

the go-ahead for the development of the mobile application. And with respect to the whole community

cation and contacts that he claims to have had with the MSND does not provide any evidence either.

guna, not even an email.

In any case, these “indications” to which he alludes are not enough to articulate the

relationship between the person responsible and the person in charge of the treatment, a relationship that cannot be

considered as a mere administrative formality or as an exchange of opinions

but as a means to seek the defense and protection of the Fundamental Law

critical to the protection of personal data, especially when the relationship is

established between the bodies of the same Public Administration or between different Ad-

Public administrations to whom it corresponds "to promote the conditions so that the

freedom and equality of the individual and of the groups in which he is integrated are real and

effective; remove the obstacles that prevent or hinder its fullness and facilitate the participation

participation of all citizens in political, economic, cultural and social life",

Article 9.2 of the Spanish Constitution.

In conclusion, the existence of the instructions received from the res-

responsible for the treatment, in the terms described above, unknown

their content, scope, issues, dates on which they were supplied, or what has been

the action, response and report provided by SEDIA, as a consequence of these.

In any case, even if informal communications between the

parties to provide instructions, we must mean that article 28.1.a) of the

RGPD imposes that the instructions that govern the relationship between controllers and processors

treatment outcomes are documented. And it is that, the instructions to the

that the RGPD mentions are still internal documents with effects on the re-

relationship between the controller and the data processor within the framework of a contract

treatment manager; treatment manager contract or other legal act

co which does not exist in the present case.

Therefore, it is not accredited by SEDIA that it acted following

MSND instructions.

B) Regarding the SPECIFIC ALLEGATIONS:

B.1 Regarding the processing of personal data.

It refers to the fact that the right to data protection is not absolute and invokes article 3

of the Civil Code. It argues that the requirement and application of the regulations for the protection of

data in such special and atypical circumstances, must be balanced and weighted

and that the Agency cannot act as if the state of alarm had not existed.

do.

In this sense, the fundamental right to data protection is not suspended by

the mere declaration of a state of alarm, but this suspension is limited

to the cases of declaration of a state of emergency or siege, as established by the

article 55.1 of the CE. In the state of alarm, only the exercise of

rights, but not suspend them.

In this specific case, the state of alarm was declared, which did not mean, in any

In some cases, the suspension of fundamental rights.

In addition, the personal data protection regulations (RGPD) itself contain the

safeguards and rules necessary to legitimately allow data processing.

personal cough in situations, such as the one that occurred, in which there was an emergency

general healthcare.

He also argues that the data was not real (they were test), that the codes of con-

tagged for introduction in the App were false and that when the App was opened in

La Gomera to the public, people could not enter real data of being infected-

two. Specifically, this allegation will be analyzed in FD V of this Resolution.

tion.

Invokes the legality of the treatment and refers to the Report of the AEPD 17/2020, of 12

March, highlighting the basis related to articles 6.1.d) and 6.1.e) of the RGPD. Effective-

mind, the data processing must be based on a lawful cause (article 6 RGPD)

and it must be transparent for those affected (articles 13 and 14 of the RGPD). Therefore, the

lack of information or transparency implies a breach of the principles of

Data Protection. This aspect will be analyzed in FD IX of this Resolution.

B.2 Regarding the role of the SGAD in data processing

1st. The stage in which the pilot project is done.

It refers again to the approval received on June 9, 2020 by the Di-

General Directorate of Public Health (sic) of the MSND where it is considered the responsibility

responsible for the processing of the pilot's data to the health authority of the Community in

that it was going to take place. We will analyze these facts in FD VII of this Resolution.

tion.

Regarding the following statement made by SEDIA: "Since SEDIA remains as

responsible for processing the data and results", nothing is said about it in the

mandate received on June 9, 2020.

This Agency agrees that the participation of the DGSP, previously

tes GENERAL DIRECTORATE OF PUBLIC HEALTH, QUALITY AND INNOVATION, in the

weekly meetings of the pilot to define the ends and means of the project.

unto Similarly, the same statement can be made regarding the participation of

the SEDIA.

And, although the data related to health handled in the pilot were simulated data

of infection (non-real data), personal data was processed, an issue that will be

rrolled in the FD V of this Resolution.

2º.- The stage in which the application is launched in the testing phase and post-

riorly the ultimate app.

It refers to the Agreement of the Interterritorial Council of the National Health System, of 19 August 2020, which allowed the Autonomous Communities to temporarily assume, until the signing of the agreements, the management of the positive diagnosis codes and the route presented by the President of the Government to deal with the rise of the "se-second epidemiological curve", which among other measures cited, the reinforcement of the media digital tracking, asking citizens to use RADAR COVID. adduces

that, in the Agreement, of October 9, 2020, which empowers the SGAD to subscribe Agreements with Autonomous Communities and Cities, the following is specified-te: "in the aforementioned collaboration agreements, the Ministry of Health and the Con-Ministry competent in matters of health of the Autonomous Community or City of in question will appear as responsible for the processing of personal data.

nal and the SGAD as the person in charge of the treatment." And specifies part of the attributions tions that according to their condition, compete to some and to others.

Nothing new contributes this allegation that was already the object of a detailed analysis in the motion for a resolution (FD VII) and which will again be refuted in FD VII of this Resolution.

The AEPD does not agree with the statement made by SEDIA regarding the existence of It has been fully accredited that at all times and in accordance with the legally binding instruments, the SGAD acted solely and exclusively as an entity charged with the treatment, because it is not until the agreement of the Agreement of the

Interterritorial Council of the National Health System, of August 19, 2020, when

do, for the first time, this condition is recognized.

In addition, according to proven fact twenty-seven, the first version of the

EIPD, of August 12, 2020, regarding the roles of “Responsible, correspondent-

responsible and in charge of the treatment” provided:

In this case, the owner of the application is the General Secretariat of Administration.

Digital transformation dependent on the Ministry of Economic Affairs and Transformation

Digital Information, which is also constituted as Responsible for the Treatment

I lie.

The application has been developed through the Secretary of State for Digi-

talization and Artificial Intelligence (SEDIA).

On the other hand, SEDIA has provided two links that lead to two documents of the

MSND:

1. Strategy for early detection, surveillance and control of covid-19.

2. Implementation procedure of the Radar COVID app as a complement

promotion of manual contact identification systems, coordinated by

the Coordination Center for Health Alerts and Emergencies, General Directorate

General Public Health, Quality and Innovation and approved by the Conference of

Alerts and Preparedness and Response Plans.

And he insists that, at all times, both in the development of the pilot, and in the use of

RADAR COVID in tests by the CCAA, and in its use, once said test phase has been

bas, the roles of controller and processor were defined, and it refers

again, to the letter of June 9, 2020, to the Agreement of the Interterritorial Council and to the

Agreement published in the BOE on October 15.

In relation to this argument, we refer to the foregoing. THE SEDIA

does not appear as in charge of the treatment until the Agreement of the Con-

interterritorial Council. The GDPR lists the elements that must be established in the

contract or legal act (article 28.3 RGPD). However, the agreement of the In-

territorial only had: The person in charge of the treatment will be, in both cases,

the Secretary of State for Digitization and Artificial Intelligence. That is, it did not stipulate

no other more specific and concrete information on how the requirements would be met.

requirements of the agreement. Subsequently, based on the Agreement published in the BOE on 15

October, the one that will appear as in charge of the treatment will be the SGAD.

In short, SEDIA appears as the person in charge of the treatment from the Agreement

of the Interterritorial Council and exercises this condition until the holding

of the corresponding agreements with the CCAA, in which it will assume the condition of

in charge of the treatment, the SGAD.

Regarding SEDIA's disagreement with some of the statements made

by the Agency regarding the METD Press Releases, since they do not attribute

no competence, this issue is not discussed by the Agency.

Article 2.1 of Law 50/1997, of November 27, of the Government provides: The President

dente directs the action of the Government and coordinates the functions of the other members

thereof, without prejudice to the competence and direct responsibility of the Ministers

in its management.

Likewise, article 3.1.d) of Law 3/2015, of March 30, regulating the exercise

of the high position of the General Administration of the State, applicable to the members of the

Government and the Secretaries of State, provides for the observance of the principle of transparency

reference and responsibility in the following terms: they will adopt their decisions in a

transparent and will be responsible for the consequences derived from its adoption.

tion.

On the other hand, the LRJSP, in article 3.1.c) provides that the Public Administrations

cas must respect a series of principles in their actions and relations, among them, the

transparency of administrative action.

Likewise, Law 19/2013, of December 9, on transparency, access to information

public governance and good governance, in article 26 under the heading “Principles of good governance”.

government”, provides that the persons included in its scope of application (members

government officials, Secretaries of State, other senior officials of the AGE, etc.) in addition to

will conform their activity to the “Principles of action”, among them, the one foreseen in the section

do 7º that refers to the performance of its functions with transparency.

In sum, the press releases, beyond being considered, according to SEDIA,

as “simple announcements made by the METD to inform citizens and

god of communication, of activities that were planned or in progress

tion”, disseminated information by the METD, facilitating knowledge by the

citizenship of the information related to contact tracing and the decisions adopted

give about it.

They are, therefore, one more proof of the activity carried out by SEDIA in relation to

with the COVID Radar app.

Regarding the fact that it was the Government that promoted the creation of this application and urged

the population to the use of RADAR COVID, it should be noted that, article 97 of the Constitution

Constitution attributes political and executive functions to the Government, a binomial that has its

reflected in all government action and that is also projected on the community relationship

nicative that in a democratic system exists between the rulers and the ruled.

The Government is undoubtedly the subject and object of information and political assessment;

but, as the ultimate person in charge of the General Administration of the State (in the

successively, AGE) and precisely because of the executive function that constitutionally

entrusted to you, is the issuer of a series of messages addressed to citizens

that are included under the generic name of institutional advertising campaigns.

and communication, as stated in the explanatory statement of the Law

29/2005, of December 29, on Publicity and Institutional Communication.

SEDIA rejects the Agency's interpretation of its role with regard to citizenship.

and alleges that he simply contributed, in collaboration with the entire Government, to

provide solutions in the field of its powers to promote the digitization of

public administrations (and all this, without taking into account the existence of categories

legal entities such as those responsible for and in charge of data protection treatment

data difficult to grasp for the common recipients).

Well then, the legal categories to which he refers are legal concepts determined

mined in article 4.7) and 4.8) of the RGPD and play a crucial role in the application

tion of the RGPD, since they determine who is responsible for compliance with the dis-

regulations regarding data protection and how interested parties can exercise

their rights in practice.

Regarding that, due to the fact of collaborating, promoting and having a relevant role in in-

try to convince the population of the use of RADAR COVID and offer explanations of

the characteristics of the application in the media, can not lead to

the conclusion that another role different from the one assigned in the do-

documents repeatedly mentioned, we refer to the provisions of the Guidelines

07/2020 on the concepts of "data controller" and "processor"

tion” in the RGPD, which in section 25 says:

“In the absence of responsibility for the treatment derived from provisions

legal requirements, the qualification of a party as a "controller" must

be established on the basis of an assessment of the factual circumstances

in which the treatment takes place. To reach a conclusion about whether a

particular entity exerts a determining influence in relation to the treatment

of the personal data in question, all circumstances must be taken into account.

pertinent facts of fact.”

And the circumstances in fact refer us to the same starting point. That is, when treating

processing of personal data by SEDIA during the execution of the project

lotto, without having a contract or other legal act that linked it with the Directorate

General Public Health, Quality and Innovation, as required by current regulations.

In this sense, section 102 of Guidelines 07/2020 says:

“Furthermore, the contract or other legal act under Union Law or

of the Member States must bind the processor against the controller;

that is, it must impose binding obligations on the processor under the

law of the Union or of the Member States. You must also set the

duties of the manager. In most cases, there will be a contra-

but the Regulation also refers to "another legal act", such as

a national rule (of primary or secondary law) or other legal instrument

co. If the legal act does not include all the minimum content required, it must include

supplemented with a contract or other legal act that includes the elements that

missing.”

B.3 Regarding the role of INDRA

It alludes to the fact that SEDIA, in its capacity as data processor, counted from the

first moment, with the authorization of the MSND, as the data controller,

for the contracting of INDRA, which had sufficient guarantees to guarantee

ticize the application of the RGPD.

Regarding this allegation, it should be noted that the proposed resolution does not impose

bitch the infringement of article 28.1 of the RGPD.

B.4 Regarding Impact Assessments

It insists that, although the EIPD published in September 2020 was version 1.1, it already

version 1.0 existed prior to August 19, 2020. The DPIA provided to

the AEPD was version 1.1 because it is the one that was published, coinciding with the deployment

in September 2020 of a version of the application, with support for co-official languages

them.

He argues that, during the period from August 19 to publication in September

In September 2020, there was an internal debate on whether or not to publish it.

It invokes the sole legal personality of the AGE; adds that, holds the status of

responsible and in charge of the treatment through different bodies and does not come

publishing neither the EIPD, nor the Risk Analysis on which they are based, of the systems

more than develop

He reasons that the SGAD sought criteria from the METD's data protection delegate. Their

The criterion was that, in general, these documents should not be published.

In any case, it finally published the DPIA and the Risk Analysis in September

2020.

On the other hand, it questions the criterion of the AEPD, page 189 of the resolution proposal.

tion, which qualifies as "more reprehensible" the lack of implementation of the EIPD at the time

timely and insists that at that time, during the pilot project, they used

simulated data, and although it was done at a time after the start-up

pilot, it was done prior to the moment in which the application was going to handle

jar user health data.

In this sense, the EIPD is a preventive tool that must be carried out

the data controller to be able to identify, assess and manage the risks to

those who are exposed to their treatment activities with the aim of guaranteeing

the rights and freedoms of natural persons.

In fact, another of the circumstances that identifies SEDIA as responsible for the

treatment, is that, through the SGAD, it was the body of the METD, in charge of cele-

Open the “Hiring Agreement” that had the purpose of hiring the services

of design, development, pilot and evaluation of a system that allows the traceability of

contacts in relation to the pandemic caused by COVID-1, an aspect that developed

we called in the FD VIII. Confirms this fact, the “Condition specifications for the design,

development, pilot and evaluation of a system that allows the tracing of contacts in re-

relationship with the pandemic caused by COVID-19” dated June 10 and 12,

2020, which requires/orders a series of deliverables, including the DPIA.

B.5 Regarding the conditions of use and privacy policy

It refers to the fact that the first version of the App (pilot) was used to check aspects

such as usability, perception of privacy, and effectiveness of the solution in an en-

simulated lathe.

It also included a notice about voluntary participation in a pilot experience

with fictitious COVID-19 infection alert data on the island of La Gomera.

He adds that the documents have been reviewed and updated with the aim of improving

rar its content and facilitate its reading and understanding, making use of its faculty of

proactive responsibility.

And that with each update of the application, consent was requested again

users express.

Regarding those responsible for the treatment, it refers to the current Privacy Policy.

(https://radarcovid.gob.es/politica-de-privacidad) that establishes as responsibility

responsible for the treatment to the MSND and CCAA, and as in charge of the treatment to the SGAD.

It justifies the increase of the 700 words with the more extensive explanations, as well

such as the extension to new uses of the application, or the interoperability with the applications

contact tracing cations of the European Union, which has led to its updating

tion, in order to provide transparency and information to users.

Remember that the Terms of Use and Privacy Policy have always been

accessible to interested parties, both from the mobile application and from the web

http://radarcovid.gob.es.

He adds that he has not received any complaint from the data protection delegate of the

MSND and that in the FAQ section of the website: https://radarcovid.-

gob.es/faq-datos-personales-y-privacidad, certain information is collected.

Well, it is true that it collects the information it claims, which is also made visible

with 16 vignettes, when in reality there are 9 aspects reported. The GDPR details the

information that must be provided to the interested party in the initial phase of the treatment, in the

Article 13, which contemplate the categories of information that must be provided to

interested parties when the data is obtained from it. This information has the character

ter of basic (article 11.1 LOPDGDD) and must be provided in a concise, transparent

clear, intelligible and easily accessible.

From the proven facts, the conclusion is drawn that the transparency of the information

Training provided throughout the various implementation phases of the pilot project

and the Radar COVID application, has been confusing, verbose and contradictory, observed

from the different sources that it emanated.

In fact, in February 2022, the contact details of the

data protection officer (hereinafter, DPD).

One of the keys to being able to guarantee privacy is being able to demonstrate it, verify it,

Do that the treatment is consistent with the information provided. data transparency

is established as a pillar to demonstrate diligence and proactive responsibility before

the control authority and as a measure of confidence before the subjects whose data is

treated. As established in recital 39 of the RGPD, for natural persons

it must be absolutely clear that they are being collected, used, consulted or processed.

otherwise using personal data that concerns them, as well as the extent to which

that said data is or will be processed.

Lastly, other factual circumstances that identify SEDIA as res-

responsible for the treatment, is that the SGAD was identified as the owner of the application,

and it was this that defined the content of the Conditions of Use and the Privacy Policy.

application city. Let us remember that it is the data controller who must

adopt internal policies and apply measures that comply in particular with the principles of

data protection by design and by default (considering 78 RGPD).

B.6

Regarding the vulnerabilities detected

He reasons that the scenario in which the vulnerability could be exploited was considered very remote.

ity, with a third party with sufficient capacity to spy on communications networks and

to cross the information sent by RADAR COVID, which would allow establishing a

relationship between the identity of the user and their positive medical condition for COVID-

19.

He argues that this judgment was correct, since it has not been detected nor is there any evidence

evidence that this theoretical vulnerability has been exploited or taken advantage of and that

there is no computer system that is 100% secure, and for this reason, it was decided, once

Given these circumstances, to continue development.

The fact that the vulnerability was corrected does not mean that the violation was not committed.

would put

Any application that is going to use personal data must be conceived and designed

starts from scratch identifying, a priori, the possible risks to the rights and freedoms

of the interested parties and minimize them so that they do not materialize in damages.

It is worth bringing up, again, the "Background" of the "Tender Specifications for

the design, development, pilot and evaluation of a system that allows the tracking of con-

tacts in relation to the pandemic caused by COVID-19" dated 10 and 12

June 2020, which read as follows:

"Being of general interest for the Government of the Nation to respond to the objective

common objective of contributing to the management of the occasional health crisis

given by COVID-19, the Secretary of State for Digitization and Intelligence

Artificial

of the Ministry of Economic Affairs and Digital Transformation, through

-

through the General Secretariat of Digital Administration (SGAD hereinafter),

activities for the definition and construction

will develop a set of

of a system

that enables close contact tracing (securely

and anonymous to the user) and its subsequent evaluation through a pilot

In relation to enabling technologies for contact tracing, there are

It should be noted that Apple and Google, companies that manage the operating systems

vos installed in practically all mobile devices worldwide,

announced on April 10, 2020 an alliance to create an integrated system

interoperable, integrated into the iOS and Android operating systems, for monitoring

contacts, which does not use geolocation but Bluetooth low energy.

gy (Bluetooth LE or BLE), to identify devices present at a distance

next.

The Apple/Google approach is based on the DP-3T protocol, which preserves

privacy through the use of ephemeral identifiers on which no

Reverse engineering is possible to obtain personal data from the owner.

device owner. Apple and Google released the developer kit (SDK,

https://apple.com/covid19/contracttracing) on May 20, which allowed

States to develop contact tracing solutions on

the new functions incorporated in their operating systems, always under the

tutelage of the national health authorities.

The System to be developed through this contract will make use of this

SDK, on which a mobile application will be built to enable the system to be activated.

contact tracing issue; that in connection with the health authorities

can receive a confirmation code of positive in COVID-19; and what-

via a server platform (backend) with which the application communicates.

mobile tion can be alerted to people with whom you have had a contact

narrow recently.

This fact points once again to the fact that SEDIA determined part of the essential media

of treatment when deciding to use Bluetooth technology following the model des-

centralized based on the DP-3T protocol.

In this sense, Guidelines 07/2020 in section 40 indicate:

As far as the determination of the means is concerned, a distinction must be made between the

essential and non-essential resources. Essential means are reserved

traditionally and inherently to the data controller. It is-

These must be compulsorily determined by the data controller.

although the determination of non-essential means can also leave

be in his hands. Essential media are tightly bound media

the purpose and scope of the processing, such as the type of personal data processed

(“what data will be processed?”), the duration of the treatment (“how long will

process?”), the categories of recipients (“Who will have access to the data?

data?”) and the categories of interested parties (“to whom do the personal data belong?

nals treated?»). In addition to being related to the end of the treatment, the

essential means are closely linked to the question of whether

the processing is lawful, necessary and proportionate.

III. CONCLUSION OF THE ARGUMENTS BRIEF

SEDIA alludes to the fact that it is aware that there may be discrepancies in the criteria

on the actions in which the work of starting up the

a necessary application in the context of a pandemic, with a state of emergency

declared. He adds that he has always acted with proactive responsibility, collaborating

with the AEPD in everything requested.

In fact, he alleges that he requested a report from the AEPD at the time it was scheduled

the extension of the application to the Autonomous Communities in August 2020, at which time

The contribution of the AEPD would have been very valuable, but the beginning of the preliminary actions

vias, determined, in the opinion of the AEPD, the impossibility of having this report.

He insists that the emergency situation and the declaration of the state of alarm altered the

ordinary legal order and the usual way of acting of the Administration.

The exceptional situation determined a modulation in the administrative procedures

administration and demanded to act quickly in order to be able to arrive on time and that the application

tion fulfilled its purposes.

The pertinent evaluations were made, the analyzes that allowed the haste with which

the application had to be developed and it was always acted with the ultimate goal of exercising

develop a proactive responsibility to allow adequate respect for the protection

of personal data.

In short, according to the previous arguments and reasoning, SEDIA

considers that there is no place for a warning sanction, because there has been no

flagrant, conscious and deliberate compliance with data protection regulations

and of all the articles that are cited in the proposed resolution of the sanction file.

tioner.

Regarding the conclusions reached by SEDIA, the following should be noted:

The personal data protection regulations, insofar as they are aimed at safeguarding

a fundamental right, was applied in its entirety during the declared state of alarm.

degree, since it did not produce the suspension of any fundamental right, being the

position adopted by this Agency in close collaboration with all the authorities

public entities that have requested their prior advice during the pandemic,

with the Ministry of Health, the AEPD having offered its collaboration in

different occasions to SEDIA, via email, on May 7 and 8, 2020, interestingly

by the working group in which SEDIA participated to coordinate with the

CCAA the deployment of the application.

So much so, that on April 7, 2020, the AEPD informed, at the request of the Directorate

Secretary of the Cabinet of SEDIA, on the standard Agreement with the Autonomous Communities

more for the development of the "APP" coronavirus application. On said Agreement also

Report 030/2020, dated April 6, 2020, was also issued. All these reports

were requested prior to the development of the applications, without there being

previous actions initiated by this Agency.

On the other hand, SEDIA alleges that it requested a report from the AEPD at the time that

the extension of the application to the CCAA was planned in August 2020, when

in which the contribution of the AEPD would have been very valuable, but the start of the actions

previous assessments, determined, in the opinion of the AEPD, the impossibility of having this information.

form. As SEDIA is well aware, comments were provided to the draft

of "Agreement between the Secretary of State for Digitization and Artificial Intelligence and

the Ministry of Health of the Autonomous Community of….on adherence to the use

of the RADAR COVID19 application", as she admits in the letter dated September 1,

December 2020 in which they respond to a request for information dated August 18,

2020 (notified on the 29th of the same month and year). However, it should be qualified

that said observations made by the Legal Office do not refer to the object

of this sanctioning procedure, but are related only to the

draft of the aforementioned agreement.

Finally, regarding the alleged emergency situation, due to the principle of

legality, in accordance with article 9 of the Spanish Constitution, citizens and

Public powers are subject to the Constitution and the rest of the legal system, without

that there was, as has been indicated, a suspension of the fundamental right to

protection of personal data, as early indicated by this Agency in its in-

form 17/2020.

IV. SUPPLEMENTARY CONSIDERATIONS

Regarding the request for the practice of the test consisting of making available

the SGAD of the following documentation that is considered essential for the

exercise of the defense in the sanctioning procedure:

a) Proposed resolution of the Instructor in relation to the procedure

opened against the MSND, in order to assess the criteria of the AEPD in relation to

the activity carried out by said department which, although it enjoys the same

legal personality that SEDIA is treated by the AEPD as a separate entity

red.

b) Full reports of the Legal Office of the AEPD cited that are cited in

the Ninth Legal Basis (17/2020 and 32/2020) of the Proposal for

Resolution, to be able to appreciate it as a whole and accept or refute it according to

be your discretion.

The request for evidence practice made by SEDIA in its office must be rejected.

letter of allegations -also requested ex officio to a party-, and this to the extent that, the

SEDIA did not formulate any proposition of proof at the relevant procedural moment.

namely, his pleadings brief filed on November 22,

2021.

It is necessary to underline that in the course of the procedure, SEDIA already benefited from

an extraordinary trial period for a period of ten additional days to the initial 30

cially granted. That is, the test practice covered the maximum period allowed

regulated by the LPACAP (article 77.2).

On the other hand, although SEDIA and the MSND act to fulfill their purposes

under the umbrella of the single legal personality of the AGE, it is organized in Pre-

Government and Ministries, each comprising one or several

various functionally homogeneous sectors of administrative activity (article 57.1

LRJSP).

In turn, each Ministerial Department has a structure of superior bodies

managers and directors provided for in Royal Decree 139/2020, of January 28, which assume

a certain bundle of competences that will be analyzed in the FD VII.

The Judgment of the Supreme Court (STS) 5298/1994, of July 9, 1994, indicates:

"…the sanctioning power of the Administration enjoys the same nature

than criminal power, so consequently, the structural guidelines

administrative offenses also tend, as in criminal offenses, to achieve the

individualization of responsibility, prohibiting any attempt to build

an objective responsibility or based on the simple relationship with a thing, for

not enough

consequently in the field of

that the conduct is unlawful and typical, but it is also necessary that

to its

is guilty, that is, as a result of an action or omission

Author

by malice or recklessness, negligence or inexcusable ignorance (STC,

Room of article 61 of the Organic Law of the Judiciary, of November 6

of 1990)"

administrative responsibility

chargeable

For this reason, even though SEDIA acts with a single legal personality, according to the principle

principle of responsibility provided for in article 28 of the LRJSP:

"They may only be sanctioned for acts constituting an administrative infraction.

natural and legal persons, as well as, when a Law recognizes them

capacity to act, affected groups, unions and entities without personal

legal purpose and independent or autonomous estates, which result

responsible for them by way of fraud or negligence."

However, the mode of attribution of liability to legal persons is not

corresponds to the forms of willful or reckless guilt that are imputable

ble to human behavior. Thus, in the case of offenses committed by

legal persons, although the element of guilt must concur, it is

necessarily applied differently from the way it is applied to natural persons.

case

According to the STC 246/1991 "(...) this different construction of the imputability of the auto-

ria of the infraction to the legal person arises from the very nature of legal fiction

to which these subjects respond. They lack the volitional element in the strict sense.

but not the ability to break the rules to which they are subject.

Capacity for infringement and, therefore, direct blame that derives from the legal right

co-protected by the rule that is violated and the need for such protection to be

really effective and for the risk that, consequently, must be assumed by the legal entity

which is subject to compliance with said rule" (in this sense STS of 24 November

November 2011, Rec 258/2009).

To the above must be added, following the judgment of January 23, 1998, partially

transcribed in the SSTS of October 9, 2009, Rec 5285/2005, and of October 23,

October 2010, Rec 1067/2006, that "although the culpability of the conduct must also

also be tested, must be considered in order to assume the correspondence

tooth load, which ordinarily the necessary volitional and cognitive elements

to appreciate it are part of the typical behavior tested, and that their exclusion

requires that the absence of such elements be proven, or in its normative aspect,

that the diligence that was required by the person who alleges its non-existence has been used; No

suffices, in short, to exculpate a typically unlawful behavior.

with the invocation of the absence of guilt".

Regarding the complete reports of the Legal Office requested, the report

032/2020 was sent to SEDIA on Tuesday, April 7, 2020 at 10:56 p.m. via mail

www.aepd.es

C/ Jorge Juan, 6

28001 – Madrid

sedeagpd.gob.es

160/212

email and was addressed to:

A.A.B. <***EMAIL.1>;

Z.Z.Z. <***EMAIL.2>

Regarding report 17/2020, it is available on the AEPD website: https://

www.aepd.es/es/documento/2020-0017.pdf.

Based on the foregoing considerations, the allegations are dismissed.

v

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": any information about an identified natural person or

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

person whose identity can be determined, directly or indirectly, in part

cular by means of an identifier, such as a name, phone number,

identification, location data, an online identifier, or one or more elements

elements of physical, physiological, genetic, psychic, economic identity,

ca, cultural or social 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 an identified or identifiable natural person;

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 enter

download access codes.

• Incorporate a factor unrelated to the operation of the application itself in the event

national deployment.”

Similarly, it has been found 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.

personal, which includes the identification of a natural person directly or indirectly.

In this sense, the STJUE of October 19, 2016, in case C-582/14, Patrick

Breyer and Bundesrepublik Deutschland, clearly provides that “The use by the legislator

Union representative of the term 'indirectly' shows that, in order to qualify a piece of information

information of personal data, it is not necessary that said information allows, by itself,

identify the interested party.

At the national level we will cite for all the SAN of March 8, 2002 in which

indicates that “for a personal data to exist (as opposed to data

dissociated) a full coincidence between the data and a person is not essential

but it is enough that such an identification can be effected effortlessly.

disproportionate risks” and “to determine if a person is identifiable, it is necessary to

consider all the means that can be reasonably used by the

responsible for the treatment or by any other person, to identify said person.

sound”.

For such purposes, we must take into consideration the opinion of the Working Group

of article 29, today replaced by the CEPD, 4/2007 on the concept of personal data

in which it is stated that “a natural person can be considered «identified»

ca when, within a group of people, he is "distinguished" from all the others

group members".

Recital 26 of the RGPD prevents a series of criteria to decree if a person

natural person is or is not identifiable: “To determine whether a natural person is identifiable

possible, all means, such as singling, that reasonably

can probably be used by the data controller or any other person to

directly or indirectly identify the natural person. To determine if 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 the costs and the time required.

necessary for identification, taking into account both the technology available in the

time of treatment and technological advances.

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 CEPD Guidelines

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 supplier

Internet access of said person.

Without forgetting that the Article 29 Group itself means that “The Working Group

treats IP addresses as data about an identifiable person. In that sense-

do has stated that “Internet access providers and administrators of

local networks can identify by reasonable means the Internet users to whom they

that have assigned IP addresses, since they systematically record in a file the fe-

cha, the time, the duration and the dynamic IP address assigned to the Internet user. It

The same can be said of Internet service providers who maintain a fi-

log file on the HTTP server. In these cases, there is no doubt that

speak of personal data in the sense of letter a) of article 2 of the Di-

rectiva””, Opinion of the Working Group of article 29, 4/2007 on the concept of

personal information.

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

identified or identifiable. Pseudonymized personal data, which could be attributed

buy a natural person through the use of additional information, they should consider

information about an identifiable natural person. To determine if a person

physical person is identifiable, all means must be taken into account, such as the

authorization, which can reasonably be used by the data controller or any other

any other person to directly or indirectly identify the natural person. For
determine whether there is a reasonable probability that means will be used to identify
caring for a natural person, all objective factors must be taken into account, such as
the costs and time required for identification, taking into account both the
technology 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.

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 private.

cularly sensitive in relation to fundamental rights and freedoms,

that the context of their treatment could entail significant risks to the rights

rights and fundamental 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.

Well, as we anticipated in the initial agreement and in the resolution proposal,

tion there were personal data involved in the analyzed treatment.

Thus, in the test practice, SEDIA determined what it called "potential-

personal mind that the application deals with",

“Generation of codes for the communication of positives in the application

COVIDRadar.

o Positive confirmation code. These 12-digit codes are

generated by the Radar COVID server using pseudo-automated algorithms.

random, and made available to the health authorities of the

autonomous communities, for distribution among confirmed cases

of COVID-19 in its territory. This number is still the "confirmation"

tion" that the user has indeed tested positive, and it is not about

a malicious user who wants to trigger false alerts. It is-

These codes are valid for a maximum of one month, after which they are

removed from the server and cannot be used for confirmation

of positives. Likewise, if a user enters a confirmation code

valid tion, once validated on the server, is also deleted.

Reception of the information sent by users when they communicate a

positive. Daily exposure keys up to a maximum of 14 days. The number-

exact number of communicated codes will depend on the date of onset of symptoms

or date of diagnosis that is reported in the application.

o IP address of the user. To the extent that Radar applications

COVID establish contact with the server, both for downloading dia-

series of keys for temporary exposure, such as for the communication of

are confirmed, the server is ready to know the address

IP used by the mobile phone to establish said communication.

In any case, this IP address is discarded, not being stored to anyone.

some effect.

o Positive communication. In the case reporting process

confirmed, the user is also asked to indicate the day on which

developed symptoms consistent with COVID-19. This information per-

allows filtering on the COVID Radar server, according to the criteria of the Ministry

rio de Sanidad, the temporary exhibition keys that are added to the

daily list of keys available to the applications. Typically

that of some days immediately prior to development will be added

of symptoms, and until the day the positive is reported. This date is

discarded after being used by the server to determine the

temporary exhibition keys that must be incorporated into the list of

diffusion.

o Temporary exhibition keys. The application generates these keys,

rate of one per day, with which the identifiers of pro-

Rolling Limits (RPI), which are exchanged between mobile phones

using Bluetooth low energy (BLE) signals. These ex-keys

temporary position are stored for a maximum of 14 days, being

removed below.

In the event that the user confirms a positive case for COVID-19

from its application, the temporary exposure keys will be communicated

to the Radar COVID server for its composition within a list

diary that can be downloaded by the set of phones with the

Radar COVID app active.

o Rolling proximity identifiers. From the exhibition keys

temporary situation, the mobile phone generates approximately every 10 minutes

mind a rolling proximity tag, which is exchanged with

other mobile phones via BLE signals. These identifiers are stored

they dine on the receiving phones, and do not communicate to any server

in any moment. They will serve to identify close contacts. I know

eliminated after 14 days.

· Composition of an updated list of temporary exhibition keys that

are made available for download by Radar applications.

give COVID.

o List of temporary exhibition keys. Once a day, the server

Radar COVID composes a list of temporary exposure keys,

composed of all the keys that have been communicated from the

Radar COVID applications whose users have reported a confirmed case

signed from COVID-19. This list is available to applications

Radar COVID, which connect daily to the server to dis-

upload that list. With the exposure keys downloaded, and cross-

ing them with the rolling proximity identifiers stored

in the mobile phone, it can be deduced according to the DP3-T protocol if

the user of this phone has been less than two meters, during

more than 15 minutes, in the last 14 days, with a person who has

A confirmed case of COVID-19 has been reported. If this is the case, the application

Radar COVID tion will warn the user of this risk situation, invi-

prompting you to self-isolate and contact the authorities

sanitary. The server maintains daily listings of exposure keys

temporary for a maximum of 14 days. The oldest listings

are removed from the system.

After that, SEDIA asserted that: "As has been stated, the data collected and

generated by the application do not allow, by default, the direct identification of the user.

rio or from your device. However, and adhering to Considering 30 of the Regulation-

European Data Protection Document, users could become identifiable

by association with some online identifier provided by the device or other

type of tools or protocols".

Likewise, SEDIA openly admits it in the EIPD of August 2020, including

between the personal data processed, among others, such as proximity data, the di-

IP address: "The IP address that the device uses to connect to the Internet. In

In this sense, it is worth mentioning the Judgment of the Supreme Court of October 3

of 2014, in which Legal Basis number four establishes that "there is no

doubt that, from the IP address can be identified directly or indirectly the

identity of the interested party, since internet access providers have constant

ence of the names, telephone and other identifying data of the users to whom they have

assigned the particular IP addresses. The Judgment confirms that the addresses

IP is personal data since it contains information concerning identifiable persons.

identified or identifiable."

The EIPD of September 2020 contains the same forecast as stated in the report

of previous actions.

Notwithstanding the foregoing, the EIPD of September 2020 states that: "The application

does not request any personal data, nor does it require creating a user (without login or da-

personal cough). The application uses anonymous keys and exchanges identifiers
Random, constantly changing. The personnel involved in the application
knows the typology of the information and, most importantly, the Security Policy".
This affirmation does not contradict what can be deduced from the proven facts, since the
that the application did not request personal data that had to be provided
by users, nor were they asked for their name, phone number or email
to be able to create a record, does not mean that there was no treatment of other data
personal.
That pseudonymized personal data were processed, as they also state, implies
ca that there is treatment of personal data.
Likewise, the fact that the pilot project worked with simulated data from
health (false positives) as asserted by SEDIA in the allegations to the proposal
of resolution, does not prevent the processing of other data
previously referenced personal data, especially when the volunteers discarded
They downloaded the application on their own mobile devices and from them they reported
positive ones.
In addition, there has been processing of personal data. In addition to personal data
previously referred to and dealt with in the pilot project, the same EIPD of August 2020 con-
creta by examining "the entire lifecycle and flow of personal data through the
treatment and all the actors and elements that intervene during the activities of
treatment from its beginning to its end" with respect to the phase of the life cycle of the
moments in which the capture of the same occurs with the "Access to in-
training stored on the mobile device at the time of installation of the
App", by users of the mobile device.
This means that with the installation of the application a treatment of
personal information.

It should be noted, at this time, that the pilot project was not closed only to

volunteers in it, but open to anyone who wanted to download the application.

tion.

SEDIA itself affirms in the evidence process that the following treatments take place-

ments, specifically and as stated in the application's privacy policy,

“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.

Reception of the information sent by users when they communicate a

positive. Daily exposure keys up to a maximum of 14 days. The number-

exact number of communicated codes will depend on the date of onset of symptoms

or date of diagnosis that is reported in the application.

· Composition of an updated list of temporary exhibition keys that

are made available for download by Radar applications.

give COVID.”

Determined, therefore, the existence of data processing is a priority

determine the role played by SEDIA with respect to the Radar CO-

VID, especially during the pilot project, which has involved the treatment of damage

personal cough. To do this, we will examine the concepts of responsible and responsible

treatment, for the purpose of elucidating whether SEDIA adapted its action to the pos-

tion that according to the RGPD corresponded to it.

SAW

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. (…)”

For its part, article 25 of the RGPD under the heading “Data protection from the di-

password and by default” 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. (…)"

Likewise, the LOPDGDD in article 28.1 states that:

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

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

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

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

present organic law, its implementing regulations and the sectoral legislation applied

cable."

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.

7th

Let us continue the legal foundation by determining and differentiating the concepts

responsible and in charge of the treatment.

Regarding the concept of "Responsible for the treatment", it is provided for in the

article 4.7 of the RGPD:

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

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

undermine the purposes and means of the treatment; if the Law of the Union or of the States

Member States determines the purposes and means of processing, the controller

treatment or the specific criteria for their appointment may establish

the law of the Union or of the Member States."

The concept of “Data Processor” is defined in section 7 of the

quoted article:

8) “in charge of the treatment” or “in charge”: the natural or legal person, autho-

public authority, service or other body that processes personal data on behalf

of the data controller;

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

that: “The RGPD has meant a paradigm shift when dealing with the regulation of de-

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

of «accountability» or «proactive responsibility» as has been pointed out repeatedly

mind the AEPD (Report 17/2019, among many others) and is collected in the Exhibition

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

personal data and guarantee of digital rights (LOPDGDD)”.

The aforementioned report goes on to say that: “…the criteria on how to attribute the different

roles remain the same (paragraph 11), reiterates that these are func-

national, which are intended to assign responsibilities according to the roles

of the parties (section 12), which implies that in most cases

The circumstances of the specific case must be taken into account (case by case), taking into account

their actual activities rather than the formal designation of an actor as "responsible

ble" or "in charge" (for example, in a contract), as well as autonomous concepts,

whose interpretation must be carried out under the European regulations on protection

personal data (paragraph 13), and taking into account (paragraph 24) that the need

The necessity of a factual assessment also means that the role of a responsible

of the treatment does not derive from the nature of an entity that is processing data.

cough but of their concrete activities in a specific context…".

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 the treatment, not losing such condition the fact of leaving a certain margin of action

tuation to the person in charge of the treatment.

This is unquestionably expressed in Guidelines 07/2020: "The person responsible for the traffic-

treatment determines the purposes and means of the treatment; that is, the why and the how of

treatment. You must decide on both the ends and the means. Nevertheless,

some more practical aspects of the treatment itself (the "non-essential means")

they can be left in the hands of the person in charge of the treatment. To be considered res-

responsible for the treatment, it is not necessary to have real access to the data that

are being treated."

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, we have

to signify the peculiar situation of the Public Administrations, where the responsible

responsible for the treatment is that administrative body that has attributed powers

by a legal norm, for whose exercise it is necessary to carry out data processing

of a personal nature. If there is no competence to carry out a certain

activity, nor does it have to carry out the treatments that are derived from it.

they would rival The jurisdiction will determine, therefore, the legitimacy to carry out the treatment.

I lie. And all this, starting from the premise that, faced with what happens in the

private sector, in which you can do everything that is not prohibited, the Administrations

Public authorities 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 Constitution)

handkerchief).

This is stated in article 8 of the LRJSP, when it is stated that "competence is

inalienable and will be exercised by the administrative bodies that have it attributed

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, and with respect to 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,
moment, who is the administrative body responsible for a competition and who is
exercising 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.

That said, according to the allegations made by SEDIA throughout the

sanctioning procedure, and for the best clarification of what happened, we can

divide the treatment related to the establishment, development and implementation of the application

Radar COVID cation in two time periods.

The first occurs from the moment in which the possibility of using

an application in order to determine the traceability of contacts, which includes

and the Radar COVID pilot project, until the “Agreement for the use of the application” is signed.

“Radar COVID” cation, in testing phase, by the Autonomous Communities

and Autonomous Cities” of August 19, 2020 of the Interterritorial Council of the System

Ma National Health. The second period begins with the validity of the Agreement of 19

August 2020. According to clause 6:

6. This Agreement will remain in force only during the testing phase

of the use of the “RADAR COVID” application and, in any case, until the signature

of the bilateral agreements of definitive adhesion for the use of the applica-

tion.

Well, there is a difference between the two periods because, as we will explain below,

tion, in the first SEDIA holds the status of data controller and in

the second SEDIA is formally designated as in charge of the treatment, all

this in relation to the Radar COVID application.

Thus, and regarding this second period, we will indicate that the performance of SEDIA

as responsible for the treatment does not dilate in time, but rather operates a change

in your condition. Specifically, based on the “Agreement for the use of the application “Radar CO-

VID”, in the testing phase, by the Autonomous Communities and Autonomous Cities

nomas” of August 19, 2020 the Interterritorial Council of the National System of

Health, as stated in the twenty-eighth proven fact, where it is indicated

that: The person in charge of the treatment will be, in both cases, the Secretary of State of

Digitization and Artificial Intelligence

Also subsequently, the Resolution of October 13, 2020, in the Clause

Third, section 2 and 3, the SGAD is recognized as in charge of the treatment, res-

aspect of the "Obligations of the parties in relation to the delegation of powers

provided for in letter b) of the first clause” in accordance with the thirtieth proven fact

I come And to the General Secretariat of Digital Health, and Innovation of the National System

of Health, in its capacity as Responsible for the treatment, give the necessary indications

sarias to the SGAD in its capacity as data processor.

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 Privacy Policy there are modifications with respect to the ver-

initial session.

The final version introduces a “Point 3” that answers the question: Who are the

responsible for the treatment of your data as a user of "Radar COVID"?, and informs

the next:

“At the national level, the person responsible for processing your data as a user of

"COVID Radar" is: (...)

Name: Ministry of Health.

Address: Paseo del Prado 18-20, 28014 Madrid

The General Secretariat of Digital Administration, as the owner of the application

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

tion and based on the order of the treatment entrusted by the Ministry of Sanita-

ity, will carry out the following treatment operations:

~

Generation of codes for the communication of positives in the application

COVIDRadar.

~

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 number

The exact number of keys communicated will depend on the date of onset of symptoms.

more or date of diagnosis that is reported in the application.

The preference or not to communicate these keys of daily exposure to the

European node for interoperability between contact tracing applications

cough.

~

~

~

Composition of an updated list of temporary exhibition keys

that are made available for download by the applications

nes Radar COVID.

~

In relation to the European contact interoperability node (EFGS)

~

Daily reception of the lists of temporary exhibition codes generated

two by the national servers of the Member States adhering to

your case to the project.

~

Daily submission to the EFGS node of a list of temporary exposure keys

poral sent by users of Radar COVID who have consented ex-

explicitly share this information with the rest of the Member States

attached to the project. (…)"

Leaving behind this second period, we will now focus on the first to determine

determine who was the data controller with respect to the processing of personal data.

in relation to the realization of the Radar COVID pilot project.

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 AEPD Legal Office N/REF:

0017/2020).

Even though there is some 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) the Minister of Health is designated as the delegated competent authority

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 time the treatment began.

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 (at the time in which the actions of the

treatment). Article 3 of the aforementioned Royal Decree contains its functions, including

leaving those related to public health surveillance or the actions contemplated in

Law 33/2011, of October 4, General Public Health, are the responsibility of the

state health administration, among others.

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 "the promotion of the digitalization of the public sector and the coordination and cooperation

terministerial and with other Public Administrations regarding said matters, without

detriment of the competences attributed to other ministerial departments".

Applying the foregoing to the case at hand and as a result of the actions carried out

developed by the METD through SEDIA and SGAD, the role that corresponded to

SEDIA according to the RGPD was the one in charge of the treatment, since the competence

ence for the treatment of personal data object of the application developed the te-

responsibility attributed to the current General Directorate of Public Health (Royal Decree 735/2020, of

August 4), before, General Directorate of Public Health, Quality and Innovation.

However, from the proven facts, it is concluded that SEDIA held the condition

of data controller since the project began in May

2020, until the Agreement for the use of the "Radar COVID" application, in the testing phase,

by the Autonomous Communities and Autonomous Cities" of August 19,

2020 the Interterritorial Council of the National Health System, mentioned above, where

SEDIA is recognized as being in charge of the treatment.

That said, and based on the fact that during the pilot project the person in charge

responsible for the treatment for being the holder of the competence was the General Directorate of Health

Public, Quality and Innovation of the Ministry of Health - admitted by SEDIA in the

allegations adduced in the course of the procedure, even indicating that he was entrusted

treatment- the truth is that, considering all the factual circumstances

relevant and that have been proven, SEDIA held the status of responsible

of the treatment. This circumstance has been proven and derives from the documentation

contained in the administrative file and the allegations made during the

penalty procedure.

Thus, the role of data controller held by SEDIA is revealed

through their own actions, both ad intra and ad extra.

Ad intra, with respect to the rest of the actors involved in the pilot project belonging to

to the Public Administration. SEDIA determined a large part of the purposes of the treatment

and decided on the essential means to carry it out.

We must start from the letter of June 9, 2020 from the General Directorate of Health

Public, Quality and Innovation. In said letter, the data controller gives the approval

good for the development of the Radar COVID pilot project through a mobile application and

also generically determines the purpose of the processing of personal data in

the aforementioned pilot project, that is, the traceability of contacts of COVID-19.

Let us clarify with respect to the allegation made by SEDIA that it remains as entrusted

from the treatment of the data and results, that the letter in relation to the roles is

limited to the following tenor: “In its authorization, the DGSP establishes June 9, 2020

that: the person responsible for processing the data of this pilot will be the health authority

ria of the Community in which it is going to be carried out”.

This is a conclusion that SEDIA seems to reach, in view of the investigation and

subsequent opening of the sanctioning procedure: first, because the reference letter-

does not mention the role that SEDIA must play, but merely gives the approval

good regarding the development of the pilot project; second, because, if as then

understood the General Directorate of Public Health, Quality and Innovation, the person in charge

of the treatment was the health authority of the Autonomous Community in which the

to carry out the treatment, it would have been up to her to designate the person in charge of the treatment through the legally established instruments and not to the Directorate General Education of Public Health, Quality and Innovation.

Notwithstanding that the General Directorate of Public Health, Quality and Innovation, gave the approval of the Radar COVID pilot project through the letter of June 9, 2020, the truth is that SEDIA was not formally determined to be in charge of the ment during the pilot project.

Nor does the mention contained regarding the "role" of SEDIA in the "Condition specifications for the design, development, pilot and evaluation of a system that allows contact tracing in relation to the pandemic caused by the COVID-19" dated June 10 and 12, 2020, in which they merely point out that:

"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 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 Development of technological solutions and mobile applications for data collection 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."

It is interesting to make a couple of points regarding 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 information, the development of new actions for the management of the health crisis

ria caused by COVID-19 (hereinafter OM).

Specifically, the First section provides:

"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

of 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

of the Ministry of Economic Affairs and Digital Transformation, the development

development of an informative website with the technological resources available."

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)).

The development of the pilot project and its implementation was not even included in

Order SND/297/2020, of March 27, entrusting the Secretariat of

State of Digitization and Artificial Intelligence, of the Ministry of Economic Affairs

and Digital Transformation, the development of various actions for the management of the

health crisis caused by COVID-19. The Radar COVID App, and therefore its pro-

pilot project, was not included within the technological solutions and applications

mobile phones for data collection in order to improve the operational efficiency of

health services.

If the MSND had wanted to entrust SEDIA with the development of the Ra-

give COVID, he would have shown his will unequivocally. And I would have done it

the same way as the rest of the parcels. However, the formal commission does not

Occurred.

SEDIA points out in its arguments that page 159 of the proposed resolution

states the following: “The AEPD does not go into neither examining nor qualifying what should be the

legal instrument through which SEDIA is formally entrusted with the assignment

of the treatment referred to the RADAR COVID pilot project. Obviously it exceeds

our competencies. Now, precisely, we highlight the delegation of com-

claims and the management entrustment among the instruments provided for in article

8.1 of the LRJSP for being the ideal ones to carry out a treatment order between

administrative gains.”

And he alludes to the fact that the instrument used, different from the encomienda, was the enabling letter.

health tea.

In this regard, it should be noted that the will of the competent administrative body is

manifested through administrative or regulatory acts, in such a way that these are re-

loved ones to formalize the task of being in charge of the treatment; which I know

complements the obligation prescribed in article 28.3 of the RGPD that specifies that

“The treatment by the person in charge will be governed by a contract or other legal act with lease.

under the Law of the Union or of the Member States, which binds the person in charge

responsible party and establish the object, duration, nature and purpose

of the treatment, the type of personal data and categories of interested parties, and the obligations

tions and rights of the person in charge".

Thus, for example, it has been made clear both in the Ministerial Order SND/

297/2020 of March 27, as in the Agreement of October 13, 2020.

With regard to who has determined in practice the purposes and means of processing,

we must mean that it has been proven that SEDIA was appointed in charge of the

Presentation at the meeting of the interterritorial working group on June 17, 2020

which was attended by representatives of various Autonomous Communities, as well as

members of SEDIA, without any presence of members of the MSND, where it was exposed

so that:

"…three main objectives of the application: preserve public health, go a

stay ahead of COVID-19 and minimize its economic impact by facilitating

the movement of people. To do this, there are three key moments to keep in mind:

account: the activation of Bluetooth (which allows to preserve the anonymity of the

users), the report of positive diagnoses and the notification to users in

risk of infection".

In addition, the application would serve the purpose of conducting online surveys "to obtain

critical mass".

To the above we must add the document called "COVID Radar. Secretary

General of Digital Administration. General operation. Madrid, June 2020" where

SEDIA reported on the objectives of the app:

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

• Be one step ahead of Covid-19: alerting people at risk is containing

the virus proactively

• Minimize the economic impact of Covid-19, by controlling the pandemic without

drastic measures and facilitating the movement of people."

Thus, when SEDIA explained the objectives of the application, it was merely delimiting the

purposes of treatment, amplifying that set by the General Directorate of Public Health,

Quality and Innovation (

; this participation in the determines

traceability of contacts)

-

The definition of the purposes implies the condition of data controller.

But it is that, in addition, it determined part of the essential means of treatment, decided

addressing issues such as, with respect to cross-border interoperability,

opt for the decentralized DP3T Protocol, which incorporates the API of Apple and Google

regional health services.

o The proposal of five models for the integration of the subsequent application in the

Likewise, through the "Condition specifications for the design, development, pilot and evaluation

Implementation of a system that allows contact tracing in relation to the pandemic

caused by covid-19", accepted by INDRA, the means of tra-

previously fixed treatment. The "celebration" of the emergency contract with INDRA,

as the person in charge of treatment, without the subsequent authorization of the real person in charge

of the treatment required by article 28.2 of the RGPD, shows that the SE-

DIA acted as data controller, deciding on the means of processing.

I lie.

We must also cite the document called "Covid-19 App Pilot Design. Pre-

CCAA statement June 17, 2020, prepared by SEDIA in which the para-

Key meters of the Pilot and the access channels by the participants.

It should be added that, of all the documentation in the administrative file

there are no documented instructions from the real data controller that justifies

verify this “excessive” action by SEDIA with respect to its role as traffic manager.

treatment.

Continuing with our argument, the initial version of the

“Radar COVID Application Privacy Policy” published on August 7,

2020 together with version 1.0 of the Radar COVID app (pilot version), where the

Next information:

“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

used during the use of 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 con- trol alert functionality.

tagos that allows to identify situations of risk for having been in contact

close relationship with users of the application who are infected

given by COVID-19. In this way you will be informed of the measures that

comes to adopt later".

In this information, the role of data controller is clearly assumed by the

SGAD.

Likewise, ad extra, through the press releases published by the METD, it is

revealed that SEDIA, from the beginning, acted as controller of the

I lie.

The first press release is published on May 6, 2020 (proven fact

sixth) where it is reported that "Spain works at a national and European level for the integration

perability of contagion prevention applications against COVID-19", highlights

playing the role of the METD together with the secretaries of state (SEDIA, included).

It is significant that this press release, dated May 6, 2020, predates the letter

of the General Directorate of Public Health, Quality and Innovation of June 9, 2020.

Likewise, on June 23, 2020, in the Reference of the Council of Ministers,

the Agreement adopted regarding the declaration of emergency for the

contracting of the services of design, development, pilot and evaluation of a system

that allows contact tracing, as stated in the tenth proven fact

fourth.

That same day, the METD publishes a press release reporting the approval by

part of the Government of the development of the pilot for a mobile application of notification of

risk contacts by COVID-19, as stated in the tenth proven fact

third.

Subsequently, on August 3, 2020, the METD publishes another press release

informing about the passing of the testing phase fulfilling all the objectives

marked. (...) This is what the Secretary of State for Digitization and Intelligence has explained.

Artificial Agency, Carmen Artigas, (...), according to the twenty-second proven fact

second.

Also, on September 9, 2020, the METD publishes another press release

where it reports that implementation is complete in thirteen autonomous communities, which

cover 70% of the population, and releases its code, according to the proven fact

thirty fourth.

Finally, on October 22, 2020, the METD publishes a press release informing

command over the commitment of the main telephone operators to not affect

reduce the data consumption of the Radar COVID app to its users. (...) And it refers to the ti-

head of SEDIA, who is the one who holds a meeting with representatives of the main

major telephone operators with the aim of establishing ways of collaboration to

the dissemination of the Radar COVID contact tracing mobile application (a proven fact

fortieth).

And although SEDIA disagrees with the value of the proposed resolution in its arguments

evidence attributed to them by the AEPD, an issue already analyzed in the FD IV, the truth is

which are one more element that has contributed to clarify the role of SEDIA in the development

application roll.

Likewise, SEDIA confirmed to this Agency -in response to the first request-,

that: “(…) it is appropriate to indicate that the app that will allow the tracking and notification of con-

tacts in order to promote the early detection of possible people infected by CO-

VID-19 is still in the design phase. At this time, there are still

many uncertainties and pending decisions, which can be elucidated

As the pilot project announced by the Third Vice President progresses and

will be held in the Autonomous Community of the Canary Islands, which will be reported

timely to the AEPD."

We also highlight the document "FAQs RADAR COVID", sent by SEDIA,

on July 21, 2020, 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.

As we pointed out before, it also pronounces regarding the purposes of the App that

are linked to the purposes of the treatment in the following sense:

"The specific purpose of the tracking application is to meet the following objectives:

you:

 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."

And there is no doubt, in relation to the determination of the means, that SEDIA is

through the SGAD, which has developed the tracking application. That's how it gets ma-

manifested in the Resolution of October 13, 2020, of the Undersecretariat, which in its

Sixth paragraph 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 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”

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

Radar COVID app respectively.

In other words, there was a real appearance to the public that it was the answer.

responsible for the treatment, despite the fact that SEDIA, in the allegations to the proposal

resolution, insists on denying this appearance, referring to the fact that it was the Government

who promoted the creation of the application and encouraged its use.

Finally, we rule out the co-responsibility of the General Directorate of Public Health.

ca, Quality and Innovation and SEDIA.

The RGPD defines in article 26.1 what it understands by "Joint controllers of the treatment-

I lie":

"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 General Directorate of Public Health, Quality and Innovation

tion and SEDIA, have jointly determined the objectives, the means of treatment,

their respective responsibilities, so the condition would be ruled out.

tion of co-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.”

The "Agreement for the use of the "Radar COVID" application, in the testing phase, by

the Autonomous Communities and Autonomous Cities” of August 19, 2020 on

Interterritorial Council of the National Health System in point 5 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

Article of April 27, 2016, regarding the protection of natural persons with regard to

respect to the processing of personal data and the free circulation of these data and for the

that Directive 95/46/CE is repealed, during the term of this Agreement, the

responsible for the treatment will be the Ministry of Health and, in its respective territory, each

one of the autonomous communities and cities that are incorporated during the

testing phase to the use of the application, fully displaying its competences in

health matter. The person in charge of the treatment will be, in both cases, the Secretary of

State of Digitization and Artificial Intelligence".

It should also be noted that the General Secretariat for Digital Health and System Innovation

National Health, in response to a request dated December 4, 2020,

inform 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, (…):

Without going into an analysis of the General Directorate's status as data controller,

Public Health, Quality and Innovation, which is evident, until it occurs

the signing of the Agreement, it has been proven that SEDIA held the condition of res-

responsible for the treatment, without having legal coverage to exercise this condition.

Consequently, it was not the competent body to process personal data.

in relation to the intended purposes, with which the lack of competition has

determined an absence of legitimacy for the processing of personal data

staff. As we stated earlier, the legitimacy to carry out a trade

treatment, in the field of Public Administrations, is inextricably linked to

the competence of the administrative body that holds it, since only the one that is the

competent authority can decide on the means and purposes of the treatment.

Furthermore, neither did it occur prior to the Resolution of 13

October 2020, delegation of any competence or management assignment that

allow the exercise of jurisdiction.

In short, as a conclusion from the foregoing, it can be stated that the SEDIA attached to the

METD, to which the SGAD depends, with the rank of Undersecretary, has served as

responsible for the data processing referred to in the factual background, all

Once in accordance with the definition of article 4.7 of the RGPD, it has determined the purposes and

means of the treatments carried out (in addition to the appearance before the citizens

as data controller).

The legal system has provided for the contingency that whoever is in charge of the

treatment behaves as responsible for the treatment. Article 28.10 of the

RGPD provides that "Without prejudice to the provisions of articles 82, 83 and 84, if an en-

charged with the treatment infringes this Regulation when determining the purposes and me-

god of the treatment, will be considered responsible for the treatment with respect to

no treatment". The consequence is also determined in article 33.2 of the

LOPDGDD when it is indicated that those who

"in their own name and without proof that they act on behalf of another, establish relations

tions with those affected".

The facts described are constitutive of the infraction foreseen in article 83.4.a) and

83.5.a) of the GDPR.

viii

It is opportune -at this moment- to bring up the legal regime related to the

loaded with treatment:

First of all, we refer to article 4.8 of the RGPD already indicated.

Second, 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."
Third, article 28 of the RGPD under the heading "Data Processor"
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

of the person in charge, including with respect to the transfers of personal data to

a third country or an international organization, unless required to do so in

under the law of the Union or of the Member States that applies to the

loaded; In this case, the person in charge will inform the person in charge of that legal 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."

Fourth, 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 the person in charge has communicated
to carry out the treatment object of order, without prejudice to the fact that it may in-
incur in an infringement of the RGPD with said action.
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.

Let us remember that according to the royal decree Royal Decree 463/2020, of March 14, the
MSND acts as delegated competent authority in its respective area of responsibility.
sability. Consequently, given that the objective or purpose of the treatment is the pre-
prevention of the coronavirus pandemic, corresponded and corresponds to the Ministry of
Health determine the ends and means to be used.

On the contrary, SEDIA - from the beginning - should have acted on the condition

of treatment manager, which is the figure in which she clearly fit

in accordance with the provisions of the RGPD, an issue that should have been implemented

do in accordance with the requirements of article 28.3 of the RGPD; however, being encar-

data subject has acted as data controller, as inferred

re of the proven facts.

Well, centered on the subject and in accordance with the above, another of the actors that intervene

come in the project is the trading company INDRA SOLUCIONES TECNOLOGÍAS

DE LA INFORMATION, S.L.U (hereinafter, INDRA).

It is the SGAD that, on June 15, 2020, agrees to contract the services

services for the development of an application for the traceability of contacts in relation to

the pandemic caused by COVID-19, to INDRA, for an amount of 330,537.52 euros.

rivers (VAT included).

The contract signed for this purpose is carried out through the emergency procedure, in

the terms of article 120 of Law 9/2017, of November 8, on Contracts of the

Public Sector, which transposes into the Spanish legal system the Directives

of the European Parliament and of the Council 2014/23/UE and 2014/24/UE, of February 26-

ro of 2014 (hereinafter, LCSP).

An exceptional regime is thus established "when the Administration has to act

immediately due to catastrophic events, situations that occur

pose a serious danger or necessities that affect the national defense". The end-

ultimate duty is to execute everything necessary "to remedy the event produced or

satisfy the supervening need", article 120 of the LCSP.

The serious concurrent circumstances in these assumptions except the need to

process contracting file in the terms of article 116 and following of the

LCSP, even excluding the existence of adequate and sufficient credit.

That is why we do not have the Specific Administrative Clauses Documents.

cular of the aforementioned contract. The Resolution of the Central Administrative Court of Re-

Contractual courses no. 906/2018, of October 5, in its legal basis

seventh, indicates that the Specific Administrative Clauses are the instrument

legal document that delimits the conditions and circumstances of unfolding

of its beginning of the administrative hiring and that constitute the law of the contract. I know

are regulated in article 120 of the LCSP.

They determine, among other issues, "the criteria of solvency and adju-

dication of the contract; the social, labor and environmental considerations that, as

criteria of solvency, award or as special conditions of execution are

establish; the agreements and conditions defining the rights and obligations of

the parties to the contract; the forecast assignment of the contract except in cases in which the

same is not possible in accordance with the provisions of the second paragraph of article

214.1; the obligation of the successful bidder to comply with the salary conditions of the workers

guarantors in accordance with the applicable sectoral Collective Agreement; and the others mentioned

tions required by this Law and its implementing regulations. In the case of mixed contracts

cough, the legal regime applicable to its effects, compliance and termination will be detailed,

in accordance with the rules applicable to the different services merged into them".

The Specific Administrative Clauses will also contain the provisions

descriptions in terms of data protection, since what is related to the development of the

contract in relation to the treatment of personal data that is entrusted to the

The person in charge of the treatment is also part of the signed contract. Being the clauses

clauses of these specifications of a legal nature, must be complemented with those of a legal nature.

technical ter of the Specifications of particular technical specifications (article 124 of the LCSP),

that will set from a technical point of view, how the project should be materially executed

administrative contract.

Set things like this, although the emergency procedure excludes the formalities

provided for in the LCSP regarding the processing of the corresponding file of

administrative contracting, does not exempt compliance with the protection regulations

of data. Where the law does not distinguish, we cannot do so, especially if what

it is about the defense of a Fundamental Right. proactive responsibility does not

is blurred in these cases, but remains fully in force, in such a way that

The person responsible for the treatment must comply with the obligations imposed by the

RGPD and the LOPDGDD.

On the date the agreement was adopted, June 2020, SEDIA acted as res-

responsible for the treatment, and must, therefore, comply with the requirements of the principle

pio of proactive responsibility and with article 28.3 RGPD.

And this, because the data controller is the one who has the obligation to guarantee

the application of data protection regulations and the protection of the rights of

interested parties, as well as being able to prove it (articles 5.2, 24, 28 and 32 of the

GDPR). The control of compliance with the law extends throughout the treatment.

lie, from the beginning to the end. The data controller must act, in

in any case, in a diligent, conscious, committed and active manner.

Acting as responsible, he should have included in the signed administrative contract, the information

training required in article 28.3 of the RGPD (object, duration, nature, purpose

of the treatment, type of personal data and categories of interested parties, obligations and

rights of the controller...), which has not occurred in the case analyzed.

And if he had acted in the capacity of person in charge of the treatment -which is the one that conform to the RGPD corresponded to him but that he did not hold-, he should have required the responsible for the treatment the prior authorization required by the RGPD in writing, before recourse to another person in charge (INDRA) to develop the entrusted service (article 28.2 of the RGPD).

Furthermore, neither in the Hiring Agreement nor in the Terms and Conditions

tions, for the design, development, pilot and evaluation of the system, an alguna that attributes to INDRA the condition of data processor. Just pickge -in general-, a Confidentiality Clause, another Personal Data Protection Clause, and another Security, all of them very abstract to which we have already referred in the report of previous actions.

Nor does it include a single reference to the data controller.

The facts described are constitutive of the infraction foreseen in article 83.4.a) of the GDPR.

IX

Let us now refer to the unequivocal position that we have maintained in the Reports of the Legal Office of the AEPD 17/2020 and 32/2020.

For the AEPD “all processing of personal data that must be carried out as a consequence consequence of the pandemic and the declaration of the State of alarm must respect the fundamental right to the protection of personal data, adjusting to the provisions RGPD, which allows… to establish specific rules regarding the exercise

of said right, adjusted to the RGPD itself, as well as to the doctrine elaborated by the

Constitutional Court when interpreting article 18.4 of our Constitution, singularly

mind regarding the principle of proportionality…” .

Therefore, from the outset, there is no impossibility to harmonize the rights and interests

users, whose protection requires little justification given the epidemiological situation.

logic that happened.

It is now time to go back to FD VI where we referred to the article

5.1 of the GDPR.

The data controller must notify data subjects and the general public

that it will treat the data lawfully, loyally and transparently and must be able to demonstrate

ensure that the treatment operations comply with the provisions of the RGPD. Keep going

alleging in the motion for a resolution that in no case were data from

health of the participants in the pilot. This statement has been clarified in

the FD V.

It also argues that the Radar COVID team has been reviewing and updating the

documents with the aim of improving their content and facilitating their reading and understanding.

Paragraph 1 of the Transparency Guidelines under Regulation (EU)

2016/679 adopted on November 29, 2017, indicates:

1. Transparency is a global GDPR obligation that applies to three areas-

fundamental cough:

1) the provision of information to the interested parties in relation to the treatment

equitable;

2) how data controllers communicate with data subjects regarding

regarding your rights under the GDPR; Y

3) how data controllers facilitate data subjects to exercise their

Rights.

Transparency is an obligation of the controller, but also a right of the

interested. Transparency ensures that data processing does not remain

hidden from them and is intrinsically linked to loyalty and the new principle.

proactive liability principle that requires processing operations to be

transparent so that data controllers can demonstrate compliance

lien of their obligations.

Recital 39 of the GDPR says:

“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.”

From the proven facts, it is accredited that the first version of the application

scheduled for the pilot program (July 2020), contained in two different documents the information

privacy training:

Terms of use:

https://radarcovid.covid19.gob.es/terms-of-service/use-conditions.html

Privacy Policy:

https://radarcovid.covid19.gob.es/terms-of-service/privacy-policy.html

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. (…)"

The information made available to the public was not provided concisely,

transparent, intelligible and easily accessible, with clear and simple language.

SEDIA was also requested in the test practice for a copy of the record of the actions

personal data processing activities carried out in the pilot project, to the

purposes of verifying compliance with carrying the RAT and pointed out that:

"As Responsible for Treatment, the Ministry of Health incorporated its Re-

record of Treatment Activities, the following treatment, available at

https://www.mscbs.gob.es/servCiudadanos/proteccionDatos/docs/RAT_MSCBS.-

pdf"

In such record of treatment activities, it appears as the person in charge of the treatment.

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

of health.

Regarding the accessibility of the Radar COVID-19 application, SEDIA argues that
The conditions of use and privacy policy have always been accessible to users.
interested, both from the mobile application and from the web http://radarcovid.go-
b.es, however, in the month of September, an action was opened by the Ombudsman
of the People against SEDIA for the lack of adaptation of the tracking application of
infections, which was not accessible, especially for people with living problems.
soft. The Secretary of State for Digitization and Artificial Intelligence recognized this
circumstance by the Twitter channel.
In this sense, the Transparency Guidelines under Regulation (EU)
2016/679 adopted on November 29, 2017 indicate in section 16:
16. Similarly, if a data controller is aware that their data
goods or services are used by other vulnerable members of society,
including people with disabilities or people with problems accessing
to the information, or are directed to them, the person in charge must take into account
the vulnerabilities of such stakeholders in its assessment of how to ensure
that complies with its obligations of transparency in relation to said interested parties.
This is related to the need for a data controller to assess
Evaluate the probable level of understanding of your audience, as indicated in the
Section 9. "In writing or by other means."
On the other hand, regarding the various revisions in the "Terms of use" and "Policy-
privacy" let us not forget, that the person in charge must observe the same princi-
pios when communicating both the initial privacy statements and in any
any material or material changes you make subsequently. adduces in the al-
tions to the motion for a resolution which, following the principle of responsibility
proactively, has been reviewing and updating the documents with the aim of improving its
content and understanding, which is not in doubt.

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 continues without informing about the identity of the data controller or

about the data of the DPD, which is not even mentioned in the Privacy Policy.

Let us refer to the 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 MSND and

the CCAAs. Likewise, the SGAD is in charge of the treatment."

In relation to the categories of data, the initial version collects information:

"− The keys of temporary exhibition (…)

− 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."

The 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 and the free

circulation of these data and repealing Directive 95/46/EC (Regulation

General Data Protection Document).

Organic Law 3/2018, of December 5, on the Protection of Personal Data and ga-

guarantee of digital rights.

Organic Law 3/1986, of April 14, on Special Measures in Health Matters

Public.

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, con-

care and coordination to deal with the health crisis caused by CO-

VID-19.

Agreement of October 9, 2020, between the METD (SEDIA) and the MSND regarding the

“Radar COVID” application.”

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.

cos and epidemiological.

Let us remember that it eliminated the basis of article 9.2.j) of the RGPD.

In fact, in the allegations to the initial agreement, it stated that: “Finally, it was indicated

Note that the application does not register users, nor does it obtain information from the device.

moving positive. Notwithstanding all of the above, it is not ruled out that in the future

carry out, by the competent organisms, analysis of aggregated data on volume

of downloads of the application, volume of infected users, or other indicators

anonymous and aggregated, for scientific research projects, always complying

data protection regulations."

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.

that SEDIA justifies in the new functionalities it offers (such as the connection

of Radar COVID to the European interoperability node) and that has led to the update

zation of the conditions of use and privacy policy, in order to provide transparency

cia and information to the users of the application.

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. (…)”

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, SEDIA, acting as data controller, did not take the necessary measures

timely to provide the interested party with all the information in the terms established

cen 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, it is necessary to act in accordance with the regulations of

data protection. The legal system already contains provisions applicable to the control

of epidemics and their spread, especially in the event of natural disasters or

human gene (considering 46, articles 6.1.e), 6.1.d), 9.2.g) and i) of the RGPD).

In fact, the state of alarm has highlighted the protagonism and relevance

of the right to data protection that reaches a substantial meaning, especially

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:

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

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 any;

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:

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 no information was included regarding the person in charge,

or the rights of articles 15 to 22. Nor in the definitive version has

including the information related to the DPO contrary to what SEDIA affirms, which

points to the existence of a link to the MSND to contact the DPD, a link that

does not exist.

The facts described are constitutive of the infraction foreseen in article 83.5 of the

GDPR, sections a) and b).

X

Let's link this last aspect with another of a relevant nature that includes the RGPD.

We refer to the legal regime applicable to the “Impact Assessment related to the

data protection” (hereinafter, EIPD) which is as follows:

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 RGPD already mentioned in the FD VI.

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 DPD, since it must be required by the person in charge

of the treatment for the elaboration of the EIPD and control its realization, according to

comes article 35.2 and article 39.1.c) of the RGPD.

In this regard, the Guidelines on Group data protection officers

of Labor of article 29, adopted on December 13, 2016 and revised for the last

once and adopted on April 5, 2017, give this figure a relevant role and

fundamental when indicating that "following the principle of data protection from the

design, to article 35, section 2, specifically establishes that the person responsible for the

treatment will “seek the advice” of the DPO when conducting an assessment of

impact on data protection. In turn, article 39, paragraph 1, letter c),

imposes on the DPO the obligation to "provide the advice requested about

the impact assessment related to data protection and supervise its application of

in accordance with article 35»”. It is important to highlight the recommendation contained

in the aforementioned Guidelines in relation to the specific functions of the DPO in relation to

tion with the EIPD, since it must check “if the impact assessment related to the

data protection has been carried out correctly or not and if its conclusions (if

to go ahead or not with the treatment and what safeguards to apply) are in accordance

with the GDPR”.

In any case, and regarding the EIPD, the Article 29 Working Group recommends

that the data controller seek advice from the DPO on the following

issues:

“ . whether or not an impact assessment should be carried out in relation to the protection

data tion;

. what methodology should be followed when carrying out an impact assessment;

. whether the impact assessment should be carried out in the organization itself or sub-

contract;

. what safeguards (including technical and organizational measures) should be applied

be taken to mitigate any risk to the rights and interests of the interested parties.

sados

. whether the data protection impact assessment has been carried out

carried out correctly or not and whether its conclusions (whether or not to go ahead with the

treatment and what safeguards to apply) are in accordance with the RGPD".

The lack of EIPD, as well as its defective, incomplete, late implementation or without the participation

cipation of the DPD supposes a violation of the principle of proactive responsibility and

of privacy by design, as well as the provisions of the RGPD on the

EIPD.

In the first requirement made to SEDIA, the following was required: Copy of the analysis of

risks on the rights and freedoms of the users of the app made on the

possible data processing and impact assessment related to data protection

to do on this initiative.

In response to this request, on June 18, 2020, it reports: "The document

The risk analysis element is under development as the process progresses.

name of the solution, not being available yet".

The Agency requests the evaluation again in a second request and will not be

until September 22, 2020, when he contributes what he communicates to us at that time.

He stated that it was a first version of the impact assessment. The second of the ver-

sions is provided on October 30, 2020. And this is because on the occasion of the procedure

test has been provided by SEDIA for the first time, a version of an EIPD

prior to those cited, dated August 2020.

Let us emphasize that the launch of the pilot project in La Gomera has been taking place since

June 29, 2020 through July 29, 2020 and nationwide, commissioning

Vice of the App 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.

SEDIA, which acted as data controller, should have drawn up a

EIPD from the beginning of the development and implementation of the Radar COVID application and, in

in any case, before the processing of personal data took place. Without em-

However, as evidenced by the proven facts, the first EIPD is from August

2020 and was developed for the purpose of launching the application nationwide. identical

data, treatments and risks are present in the phase of the pilot project that with

later without any change or event taking place except the territorial amplification

application history.

The existence of a first EIPD in August 2020 also denotes a flagrant fault.

privacy by design, since the data controller must plan

treatment and assess the risks, before the treatment itself occurs.

AC. However, there has been a processing of personal data without a minimum and

brief analysis that would indicate if personal data were being processed and what they were, in

where applicable, possible risks affecting the rights and freedoms of citizens

damage, as well as the need or not to carry out an EIPD.

To all this, we must add that, initially, SEDIA told the AEPD that

no personal data was being processed. This pri-

mere allegation before the AEPD when the first time it verifies that data was processed

personal data is in the EIPD of August 2020 as stated in the proven facts.

two.

Moreover, when asked by SEDIA in the process of testing the EIPD of the pilot project,

to Radar COVID indicates that “For the pilot project, given its characteristics of si-

pandemic simulation, no impact assessment document was generated from

data protection, beyond progressing the successive drafts of what

the dessert would be version 1.0 of the document, available on August 12, 2020".

The truth is that this initial lack of foresight shows that there was no EIPD, no

However, data processing of a nature was actually being carried out

staff during the Radar COVID pilot project. For this purpose we must mention

that to arrive at the affirmation that there is no processing of personal data, it is necessary

mandatory description to perform at least an initial evaluation of such extreme to rule out

tarlo, an issue that has not been accredited by SEDIA even after the process of

Test.

It should also be noted that it does not appear in the documentation sent to the AEPD, documents

any moment in which the advice and the obligatory participation of the

DPD in EIPD.

In relation to the realization of the EIPD of the phase of the pilot project Radar COVID,

SEDIA asserted in the evidence process that "The Data Protection Delegate

of the Ministry of Economic Affairs and Digital Transformation was not consulted with the

effects of generating the first version of the impact assessment document

to data protection, as it is not a mandatory procedure.

However, article 35 of the RGPD, as we anticipated, establishes in its section

second than "2. The data controller will seek the advice of the delegate

data protection officer, if appointed, when conducting the impact assessment

regarding data protection".

In the same sense, article 39.1.c) of the RGPD provides that the DPD has the function,

among others, to “offer the advice requested about the evaluation of

data protection impact and monitor its application accordingly

with article 35”.

Derived from the above, we can conclude that the RGPD imposes on the person responsible for the

as part of its obligations, seek the advice of the DPD when carrying out

czar the EIPD, and the DPD must also supervise the application of the EIPD.

In the same vein, the Guidelines on impact assessment relating to the protection

data (DPIA) and to determine whether the processing "is likely to involve a

high risk” for the purposes of Regulation (EU) 2016/679, adopted on April 4, 2017

and last revised and adopted on October 4, 2017 establish that it is

obliged to carry out an EIPD “The person in charge, together with the data protection delegate,

data and those in charge of the treatment” documenting the opinions and recommendations

tions of the DPD.

Although it may be true what SEDIA pointed out that there was no procedure

specific interaction with the DPO in your organization, this does not prevent you from being

request their advice, not only when deemed convenient by the person in charge,

ble of the treatment in attention to the circumstances, but obligatorily in relation

with the realization of the EIPD. And this because, in addition, as prescribed in the article

38.1 of the RGPD “The person in charge and the person in charge of the treatment will guarantee that the de-

data protection legacy participates appropriately and in a timely manner in

all matters relating to the protection of personal data.

For the sake of completeness, and for illustrative purposes only, the Guidelines on

data protection legacies of the aforementioned Article 29 Working Group, es-

establish on the EIPD and the DPD that the data controller must "Ensure

that the DPO is informed and consulted from the beginning will facilitate compliance with the

GDPR, will encourage a privacy-by-design approach and therefore should

be a standard procedure in the governance of the organization".

Notwithstanding the foregoing, SEDIA affirms that "In any case, after the

elaboration of the impact evaluation, the criterion of this evaluation was obtained by telephone.

Data Protection Delegate, on the open publication of this evaluation

of impact. The criterion provided was that there was no experience in the matter of publishing

tion of these documents.

The request for advice from the DPD was subsequent to the preparation of the EIPD and cir-

consigned to the consultation on the open publication of the EIPD, in the terms of the

article 39.1.c) of the RGPD, not on the performance of the evaluation itself, which does not

prevents a violation of data protection regulations from occurring.

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.

eleventh

Next, a brief reference to article 25.1 of the RGPD, already referred to, is appropriate.

in FD VI and X.

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.

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 the Radar COVID App.

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."

SEDIA after asserting in the practice of evidence that the data collected and generated

two by the application do not allow, by default, the direct identification of the user or

its device, prevent that "however, and adhering to Considering 30 of the

European Data Protection Regulation, users could become identifiable.

cables by association to some online identifier provided by the device

or other types of tools or protocols."

At this time we must remember the concept of personal data provided for in the

RGPD and bring up the EIPD prepared by SEDIA, in August 2020, carried out-

in attention to the presence of personal data and the treatment carried out on the

themselves.

Thus, after acknowledging the existence of personal data involved, it refers to

reference to the fact that "the application has been designed respecting, as a main premise, the

current data protection regulations and especially applying all the measures

to reduce possible risks, applying all technical and organizational measures

appropriate measures designed to effectively apply the principles of protection of

data".

However, the first EIPD they present is dated August 2020, once

that the processing of personal data had already occurred through the project pi-

lotto COVID Radar

In fact, it is openly admitted in test practice that “For the pilot project

Given its pandemic simulation characteristics, no document was generated.

data protection impact assessment process, beyond progressing

the successive drafts of what would ultimately be version 1.0 of the document, dis-

available on August 12, 2020”.

However, we must emphasize that the only change was the decision of the launch

at the national level of the application, without any substantial variation occurring in-

between the pilot project and the implementation of the final application in terms of treatment

lying of personal data.

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.

The facts described are constitutive of the infraction foreseen in article 83.4.a)

of the GDPR.

XII

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.

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, 28.3, 28.10 and 35 of the RGPD, with the al-

scope expressed in the previous FD, 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:

FIRST: IMPOSE the SECRETARIAT OF STATE FOR DIGITIZATION AND INTER-ARTIFICIAL LEGISLATION the sanction of WARNING for infraction of the following you items:

- 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.
- Article 28.3 of the RGPD, typified in article 83.4.a) of the RGPD and in the Article 73 of the LOPDGDD in section k), for the sole purpose of determining prescription periods.
- Article 28.10 of the RGPD, typified in article 83.4.a) of the RGPD and in the Article 73 of the LOPDGDD in section m), for the sole purpose of determining set 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 SECRETARY OF STATE OF DIGITALIZATION AND ARTIFICIAL INTELLIGENCE.

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

938-270122

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es