Legal cabinet

N/REF: 0032/2021

The query raises the question of "whether it would be failing to comply with the premises of the RGPD for the fact of communicating the Office of Prevention and Fight against Corruption the personal data of all citizens vaccinated without them being anonymized or although, and taking into account the regulations previously exposed, it would be coherent and sufficient to provide the anonymized data or limit it exclusively to what is strictly necessary for the purpose of the investigation initiated by the aforementioned Office, which in no case has been detailed in the request received".

For these purposes, the request for information sent by the Office for the prevention and fight against corruption of the Balearic Islands Health Service of the Balearic Islands, in order to facilitate, in relation to the vaccination protocols of the Balearic Islands against COVID-19 and the specific actions of inoculation of the vaccines, and between other requested information, the following:

2.1. Regarding each of the vaccination processes and equipment: establishment, office or premises where the vaccination was performed (residences, PAC, hospitals, clinics and others), lists of people initially planned for vaccination, persons actually vaccinated, supplied vials and rejected vials (if applicable).

2.2. Name, surnames and DNI of the vaccinated person.

23. Identification of the group to which it corresponds in the protocol of vaccination.

2.4. Day and time of the first and second dose (as long as the latter, in case it has been inoculated).

2.5. Identification of the supplied vial (numerical code).

I

As this Agency has repeatedly pointed out, in the

At the time of formulating the query, the new regime should be based on

established by 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 by repealing Directive 95/46/EC (General Regulation of

data protection, RGPD) and in Organic Law 3/2018, of December 5,

Protection of Personal Data and guarantee of digital rights.

Indeed, as indicated in the Explanatory Memorandum of Law 3/2018 "the

The greatest novelty presented by Regulation (EU) 2016/679 is the evolution of

a model based, fundamentally, on the control of compliance with another

which rests on the principle of active responsibility, which requires prior

assessment by the person in charge or by the person in charge of the treatment of the risk that

could generate the processing of personal data for, from

of said assessment, adopt the appropriate measures".

Therefore, it is the data controller who must comply

with the principles that are included in article 5 of the RGPD, among which are

finds, as seen, that of proactive responsibility, collected in its

section 2, "the data controller shall be responsible for compliance

of the provisions of section 1 and able to demonstrate it ("responsibility proactive")". And among the principles of section 1 is that of "legality", collected in its letter a), so that the personal data will be treated in lawful manner, regulating article 6 the legal bases that determine the legality of the treatment. Therefore, it is the data controller who It is necessary to determine the legal basis that can protect the treatment correspondent.

Finally, a fundamental role within this new model of active responsibility established in the General Regulation of Protection of Data will be performed by the data protection delegate, which the Regulation General regulates in its articles 37 to 39. In particular, article 37.1 a) compulsorily imposes the designation of a delegate in the cases in which that "the treatment is carried out by a public authority or body, except courts acting in the exercise of their judicial function.

In turn, article 38.1 clearly establishes that "The person in charge and the in charge of the treatment will guarantee that the delegate of data protection participate appropriately and in a timely manner in all matters relating to the protection of personal data" and article 39.2 provides that "The data protection delegate will perform his duties by providing the due attention to the risks associated with treatment operations, taking into account the nature, scope, context and purposes of the treatment".

Finally, article 39.1 enumerates the functions of the delegate of data protection, among which are "informing and advising the responsible or in charge of the treatment and the employees who deal with of the treatment of the obligations incumbent upon them by virtue of this

Regulation and other data protection provisions of the Union or of

Member States” (section a), “supervise compliance with the

provided in this Regulation, of other provisions for the protection of

data of the Union or of the Member States and the policies of the person in charge

or of the person in charge of processing in matters of personal data protection,

including the assignment of responsibilities, awareness and training of the

personnel involved in processing operations, and audits

corresponding" (section b) and "offer the advice requested

c. George John 6

28001 Madrid

Legal cabinet

about the impact assessment related to data protection and

supervise its application in accordance with article 35 (paragraph c).

Likewise, it is up to the data protection delegate to “act

as a point of contact for the supervisory authority for matters relating to the

treatment, including the prior consultation referred to in article 36, and carry out

queries, where appropriate, on any other matter” (section e).

Therefore, if the data controller has doubts about the

legal basis that can determine the legality of a certain treatment

You should consult your data protection delegate in the cases in which

that, like the present one, its designation is mandatory, who must provide the

accurate advice.

Only in the event that the data protection delegate had doubts

legal decisions on the matter submitted for its consideration that cannot

resolved with the criteria already informed by the AEPD or because it is a

new issues arising from the application of the new legal regime of

protection of personal data and that have a general scope in the

that a report that contributes to legal certainty is convenient,

said delegate may submit a query to this Legal Office, accompanying

to said consultation its own report in which it is analyzed in detail and

reasoned the questions object of consultation.

In the present case, the consultation is carried out by the Protection Delegate

of Data of the Health Service of the Balearic Islands by means of a document

brief in which it is limited to raising the doubt raised with a concise

foundation. Therefore, this Agency considers that, in accordance with the

criteria indicated, it would have been necessary a motivated and detailed analysis of

the issues raised, taking into account the nature of the consulting entity

and the entity requesting the information, as well as the regulations,

jurisprudence and applicable doctrine. However, given the general interest

appreciable in the referred query and its urgency, we proceed to the

issuance of this report.

II

Law 16/2016, of December 9, creating the Office of

Prevention and Fight against Corruption in the Balearic Islands creates, in its

Article 1, the aforementioned Office, which depends organically on the Parliament of the

Balearic Islands and exercises its functions with full independence, subject to

only to the legal system and is configured as an entity of

public law, with its own legal personality and full capacity to act

for the fulfillment of its purposes.

Its functions include, in relation to prevention,

investigation and the fight against corruption, in accordance with article 5.c).4º,

c. George John 6

www.aepd.es

28001 Madrid

3

Legal cabinet

“Investigate or inspect possible cases of irregular use or destination of

public funds, as well as conduct contrary to integrity or contrary to

the principles of objectivity, effectiveness and full submission to the law and the right”,

delimiting its functions in article 6:

Article 6. Delimitation of functions.

1. The Office for the Prevention and Fight against Corruption in

Illes Balears acts in any case in collaboration, and with the respect

to the functions that correspond to them, with other organs and entities

of the Balearic Islands that exercise powers of control and

supervision of the actions of the Government, of the administrations

public and other entities of the public sector. The regulation of

operation and internal regime of the Office will regulate the

specific procedure for action in cases of exercise of

concurrent functions with other organs.

2. The Office for the Prevention and Fight against Corruption does not have

competences in the functions and subjects that correspond to the

judicial authority, the public prosecutor's office and the judicial police, nor can

investigate the same facts that are the subject of their investigations.

In the event that the judicial authority or the public prosecutor initiates a

procedure to determine the criminal relevance of facts that

constitute at the same time the object of investigative actions

of the Office, the latter must immediately interrupt said actions and

immediately provide all the information available to the

competent authority, in addition to providing, with regard to

investigation tasks, the necessary support to the authority

competent.

3. When the investigations of the Office of Prevention and

Fight against Corruption affect the Parliament of the Balearic Islands,

the statutory entities, the insular and local administrations, the

University of the Balearic Islands and, in general, the entities that enjoy

constitutionally or statutorily recognized autonomy, will be carried out

carried out in such a way as to guarantee due respect for their autonomy.

On the other hand, article 10 develops the powers of investigation and

inspection:

Article 10. Powers of investigation and inspection.

1. In the exercise of the functions of investigation and inspection, the

Office for the Prevention and Fight against Corruption in the Balearic Islands

can access any information held by the

bodies, public bodies or natural or legal persons,

public or private, included in its scope of action. In the case of

individuals, the powers of inspection shall be limited to those

activities related to contracts, grants or

public subsidies granted. In any case, access to

information must be justified, the relationship with the

investigated activity and it must be recorded in the

proceedings.

2. The director of the Office for the Prevention and Fight against

Corruption or, by express delegation, the deputy director or the director

deputy or an official of the Office who has

assigned investigation and inspection functions can:

a) Go to any office or dependency of the

Administration or center affected by a public service to request

information, carry out on-the-spot checks and examine documents,

files, books, records, accounting and databases

data, whatever the medium in which they are recorded, as well as the

physical and logistical equipment used, accrediting the condition of

authority or agent of the Office.

b) Carry out the personal interviews that are estimated

convenient, both in the corresponding administrative dependency

as in the headquarters of the Office. The people interviewed who have or

that it can be deduced that they have some type of responsibility, they can

be accompanied and assisted by the person designated. In addition,

have the rights and guarantees established by current legislation,

including the rights to remain silent and to legal assistance.

c) Access, if permitted by current legislation, to the information

of bank accounts in which payments have been made or

dispositions of funds related to procedures of

award of public contracts or granting of aid or

public subsidies, through timely request.

d) Determine, in order to guarantee the indemnity of the data

that can be collected, that authentic copies be made of the

documents obtained, whatever the support in which they are found

stored.

Regarding the conclusion of the proceedings, article 16 provides,

fundamentally, the issuance of a reasoned report on the conclusions

of the investigation, which may include recommendations and reminders, to be

sends to the corresponding body in each case:

Article 16. Conclusion of the proceedings.

1. The director of the Office for the Prevention and Fight against

Corruption in the Balearic Islands will issue a reasoned report on the

conclusions of the investigations, which will be sent to the body that in each

appropriate case, which, subsequently and within a period of three months,

inform the director or the director of the Office of Prevention and Fight

against Corruption on the measures adopted or, where appropriate, the

reasons that prevent you from acting in accordance with the recommendations and

the reminders given.

2. If in the course of the actions undertaken by the Office of

Prevention and Fight against Corruption, there are signs that

have committed disciplinary infractions or have engaged in conduct or

presumably criminal acts, the director or the director of the Office

will communicate it to the body that corresponds in each case, as well as,

immediately, to the public prosecutor's office or to the judicial authority in case of

evidence of crime. It will also be transferred to the Audit Office

In the event that the investigations may lead to a possible

Accounting responsibility, direct or subsidiary.

3. The Office for the Prevention and Fight against Corruption can lead

reasoned recommendations to administrations and public entities

in which it urges the modification, cancellation or incorporation of

criteria in order to avoid dysfunctions or practices

administrative areas that can be improved, in the assumptions and areas of

risk of irregular conduct detected.

4. If the social relevance or importance of the facts that have

motivated the action of the Office for the Prevention and Fight against

Corruption require it, the director or the director of the Office can

present to the corresponding parliamentary committee, on its own initiative

or by agreement of the same commission, the report or reports

corresponding extraordinary

Likewise, it is expected that the conclusions derived from the action

investigator and inspector will be collected in the annual report that will be sent to

the Bureau of the Parliament, as regulated in article 13:

Article 13. Annual report.

one.

In the first three months of each annuity, the Office of

Prevention and Fight against Corruption in the Balearic Islands will elaborate

an annual report describing the set of actions

developed during the previous year, in which an analysis

of the conclusions derived from the investigative action and

inspector, and the proposal of measures that are considered appropriate,

as well as the reference to the measures or actions adopted by the

competent bodies.

Personal data that allows the identification of the individuals will not be included.

people affected unless these are public as a consequence

of a final sentence or that have been sanctioned in firm by

contravene the duty of collaboration established in article 9 of this

law. In any case, the number and type of actions must be stated.

undertaken, with the express indication of the initiated files, the

dedication, the time and resources used, the results of the

investigations carried out and specification of recommendations

Legal cabinet

and the requirements addressed to administrations and entities

public, as well as their allegations.

The memory will also contain the files processed that have

been sent to the judicial authority or the public prosecutor's office, the estimate

of the possible economic amounts claimed in court or

administrative, the variations corresponding to the management of the personnel

own and the liquidation of the budget of the Office of Prevention and

Fight against Corruption from the previous year.

The liquidation of the budget of the Office of Prevention and Fight

against Corruption in the previous year and the situation of the workforce,

with the list of jobs, they must also appear in the

annual memory.

2. The annual report will be sent to the Bureau of the Parliament of the Illes

Balearic Islands, in order to transfer it to the corresponding commission, which,

in the terms provided by the Regulations of the Parliament and prior

appearance of the director of the Office of Prevention and

Fight against Corruption, can adopt the resolutions that

consider appropriate

Consequently, the possibility of sanctioning the possible

illicit conduct under investigation, establishing a system

sanctioning in Law 16/2016 referred, exclusively, to the infraction of the

collaboration obligations imposed by it.

Therefore, the Office for the Prevention and Fight against Corruption

configured as a Public Law Entity, attached to the Parliament, to which

control of the performance of the Office and the appointment and

dismissal of its director or director, as well as the approval of the regulation of

operation and internal regime (article 7), with the initiation of

official letter of the actions “On the initiative of the Parliament of the Balearic Islands,

through the agreement of the corresponding parliamentary commission, taken at

either by two parliamentary groups, or by a fifth of the

deputies and deputies of the chamber, either at the request of a commission not

permanent investigation of the Parliament itself” (article 14.1.b).

Consequently, its legal nature would correspond to that of a

auxiliary body of parliamentary bodies, participating in political control

which corresponds to them.

Likewise, the functions that

correspond to the judicial authority and the public prosecutor's office, as recalled

clearly its Statement of Motives (“The fulfillment of the functions of the

Office is understood without prejudice to those entrusted to other bodies, to

that complements acting in different operational stages, such as the

General Intervention and institutions such as the Síndic de Greuges or the Sindicatura

of Accounts and its insular and municipal equivalents, and with exemption from the

which correspond exclusively to the judicial authority and the ministry

c. George John 6

fiscal) and provides its article 6.2: "The Office of Prevention and Fight against

Corruption does not have powers in the functions and matters that

correspond to the judicial authority, the public prosecutor's office and the judicial police, nor

It can investigate the same facts that are the object of its investigations.”

All this without prejudice to the due collaboration of the

Office with the judicial authority and the public prosecutor through communication,

when appropriate, of the result of the investigations (article 5.c) 2º and 16.2), the

interruption of the proceedings, remittance of all the information and provision

of the support that is necessary when the judicial authority or the public prosecutor

initiate a procedure to determine the criminal relevance of certain facts

that constitute at the same time the object of investigative actions of

the Office (article 6.2), in addition to being configured as an entity of cooperation and permanent relationship with the judicial authority and the public prosecutor's office (article 9.2.).

Therefore, taking into account the legal nature of the Office of Prevention and Fight against Corruption in the Balearic Islands and the functions attributed to it, this Agency considers that the data processing of personal character that can be carried out by the same are subject to the general regime contained in the RGPD and not the special regime of the Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data by the competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or of execution of penal sanctions, and to the free circulation of said data and repealing Framework Decision 2008/977/JHA of the Council, and whose The transposition rule is currently being processed in the Senate.

In this regard, we must start from what is stated in article 3.7 of the Directive that defines as competent authorities, for the purposes of the same, "all competent public authority for the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, including protection and prevention against security threats public", or "any other body or entity to which the Law of the State member has entrusted the exercise of public authority and powers for the purposes of prevention, investigation, detection or prosecution of criminal offenses or execution of criminal sanctions, including protection and prevention against threats to public safety".

In this sense, recital 11 of the Directive states that

“It is therefore appropriate that these areas be regulated by a

directive establishing the specific rules relating to the protection

of natural persons with regard to data processing

personal information by the competent authorities for purposes of

prevention, investigation, detection or prosecution of violations

criminal offenses or the execution of criminal sanctions, including the protection and

c. George John 6

28001 Madrid

prevention against threats to public safety. Between

such competent authorities should not only include authorities

such as the judicial authorities, the police or other forces and

security forces, but also any other body or entity

in which the law of the Member State has entrusted the exercise of

authority and public powers for the purposes of this

Directive. When said body or entity processes personal data with

purposes other than those provided for in this Directive, the

Regulation (EU) 2016/679. Thus, Regulation (EU) 2016/679 is

applies in cases where a body or entity collects data

personal for other purposes and proceed to its treatment for the

fulfillment of a legal obligation to which it is subject. For

example, for purposes of investigation, detection or prosecution of

criminal offences,

financial conserve

certain personal data that they themselves process and only

provide such personal data to national authorities

competent in specific cases and in accordance with the Law of the

Member state. Any agency or entity that processes personal data

on behalf of the aforementioned authorities within the scope of application of

this Directive must be bound by a contract or other act

legal and by the provisions applicable to those in charge of the

treatment under this Directive, while the

application of Regulation (EU) 2016/679 remains unchanged for the

processing of personal data by data processors outside

of the scope of application of this Directive.

institutions

the

And as this Agency already pointed out when informing the bill

of transposition of the Directive in its report 122/2018, reiterated

later in report 29/2002:

The example mentioned in recital 11 is expressive in

clearly indicate that the treatment carried out by the subject

obliged to communicate the data to a competent authority is

subject to the provisions of the General Regulation for the protection of

data and not those of the Directive, without prejudice to the fact that once

communicated the data to the competent authority will be applicable to that

treatment as established in the Directive, but without that application

implies that the obligated subject is subject to the provisions of

the latter, since the communication will have been carried out at the

protection of article 6.1 c) of the regulation.

III

Once the regulations applicable to data processing have been determined

personnel that can be carried out by the Office for the Prevention and Fight against

c. George John 6

www.aepd.es

28001 Madrid

9

Legal cabinet

Corruption of the Balearic Islands, it is appropriate to attend to the specific case, in which

They request numerous personal data related to the people who have

been vaccinated against COVID19.

For this, it is necessary to start from the consideration of the information

corresponding to the fact of vaccination as a data relative to health,

given the breadth with which such data is considered in the GDPR.

In this sense, article 4.15 of the RGPD defines as "data relating to

to health", those personal data related to the physical or mental health of

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

that disclose information about your health status;

For its part, Recital (35) Among the personal data relating to

health should include all data relating to the state of health of the

concerned who provide information about their physical or mental health

past, present or future. (...) any number, symbol or data assigned to a

natural person who uniquely identifies it for health purposes; the

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

body substance, including from genetic data and samples

biological, and any information relating, by way of example, to a

disease, disability, risk of disease, history

medical, clinical treatment or the physiological or biomedical state of the interested party,

regardless of its source, for example a doctor or other professional

healthcare, a hospital, a medical device, or an in vitro diagnostic test.

And the jurisprudence of the Court of Justice of the European Union comes

also advocating a broad interpretation of the concept, as

already pointed out the Judgment of November 6, 2003 (case C-101/01,

Lindqvist) interpreting Directive 95/46/EC of the European Parliament and of the

Council, of October 24, 1995, relative to the protection of people

physical with regard to the processing of personal data and the free

circulation of these data, in section 50:

Taking into account the purpose of this Directive, it is necessary to give a

broad interpretation of the term "health data",

used in its article 8, paragraph 1, so that it understands the

information relating to all aspects, both physical and psychic,

of a person's health.

From the foregoing, it must be concluded that the information regarding the condition

having received the vaccine, as soon as it reveals information about the state of

health of the people who have received it, is a health data, and therefore

must be included within the "special categories of data" in accordance with the

article 9 of the RGPD.

Regarding the processing of personal data corresponding to the

"special categories of data", the general rule is its prohibition, as

It is included in article 9.1. of the GDPR:

The processing of personal data is prohibited

reveal ethnic or racial origin, political opinions, convictions

religious or philosophical beliefs, or trade union affiliation, and data processing

genetic, biometric data aimed at uniquely identifying

a natural person, data relating to health or data relating to life

sexual orientation or sexual orientation of a natural person.

Therefore, the processing of special categories of data

personal must find coverage in article 9.2 RGPD and once

Except for the general prohibition, it is necessary to resort to the assumptions of the

article 6 RGPD to give legality to the treatment in question. This was already indicated by

Article 29 Working Group (whose functions have been assumed by the

European Committee for Data Protection) in its opinion “Guidelines on

automated individual decisions and profiling for the purposes

of Regulation 2016/679” when indicating that (…) Those responsible for the treatment

they can only process special category personal data if a

of the conditions provided for in article 9, paragraph 2, as well as a

condition of article 6.(…), and more recently, the European Committee of

Data Protection in its "Guidelines 03/2020 on data processing

related to health for scientific research purposes in the context of the outbreak

of COVID-19, adopted on April 21, 2020”:

All processing of personal data relating to health must

comply with the relevant principles set out in article 5 of the GDPR

and conform to one of the legal bases and specific exceptions

listed, respectively, in article 6 and article 9 of the

RGPD for the legality of the treatment of this special category of data

personal.

Therefore, the first thing to analyze is whether any of the

exceptions that lift the prohibition of the processing of data relating to

health and that are included in section 2 of article 9 of the RGPD, when indicating

which will not apply in the following cases:

a) the interested party gave his explicit consent for the treatment

of such personal data for one or more of the specified purposes,

except when the law of the Union or of the Member States

establishes that the prohibition mentioned in paragraph 1 cannot be

raised by the interested party;

b) the treatment is necessary for the fulfillment of

obligations and the exercise of specific rights of the person responsible for the

treatment or of the interested party in the field of labor law and

security and social protection, to the extent authorized by the

Union law of the Member States or a collective agreement

in accordance with the law of the Member States that establishes

adequate guarantees of respect for fundamental rights and

interests of the interested party;

c) the processing is necessary to protect the vital interests of the

interested party or another natural person, in the event that the interested party is not able, physically or legally, to give consent;

d) the treatment is carried out, within the scope of its activities legitimate and with due guarantees, by a foundation, an association or any other non-profit organization, whose purpose is political, philosophical, religious or trade union, provided that the treatment is refer exclusively to current or former members of such organizations or persons who have regular contact with them in relation to its purposes and provided that the personal data is not communicate outside of them without the consent of the interested parties;

e) the treatment refers to personal data that the interested party has manifestly made public;

f) the processing is necessary for the formulation, exercise or defense of claims or when the courts act in the exercise of its judicial function;

g) the processing is necessary for reasons of public interest essential, on the basis of the Law of the Union or of the States members, which must be proportional to the objective pursued, respect in essential the right to data protection and establish measures adequate and specific to protect the interests and rights fundamentals of the interested party;

h) the treatment is necessary for the purposes of preventive medicine or work, evaluation of the work capacity of the worker, diagnosis medical care, provision of care or treatment of a health or social nature, o management of health and social care systems and services, on the basis of the law of the Union or of the Member States or on

under a contract with a healthcare professional and without prejudice to the

conditions and guarantees contemplated in section 3;

i) the treatment is necessary for reasons of public interest in the

field of public health, such as protection against threats

serious cross-border risks to health, or to ensure high levels

quality and safety of health care and

medicines or health products, on the basis of the Law of the

Union or of the Member States that establishes adequate measures and

specific to protect the rights and freedoms of the interested party, in

particularly professional secrecy,

j) the processing is necessary for archiving purposes in the interest

public, scientific or historical research purposes or statistical purposes,

in accordance with Article 89, paragraph 1, on the basis of the Law

of the Union or of the Member States, which must be proportional to the

objective pursued, to respect essentially the right to protection of

data and establish adequate and specific measures to protect the

interests and fundamental rights of the interested party. (...).

In relation to these causes that lift the prohibition of treatment

of the special categories of personal data, the LOPDGDD contemplates

specific provisions in its article 9:

Article 9. Special categories of data.

1. For the purposes of article 9.2.a) of Regulation (EU) 2016/679,

In order to avoid discriminatory situations, the sole consent of the

concerned will not suffice to lift the ban on data processing

whose main purpose is to identify their ideology, union affiliation,

religion, sexual orientation, beliefs, or racial or ethnic origin.

The provisions of the preceding paragraph shall not prevent the processing of

said data under the other assumptions contemplated in the

Article 9.2 of Regulation (EU) 2016/679, when appropriate.

2. The data processing contemplated in letters g), h) and i)

of article 9.2 of Regulation (EU) 2016/679 founded on the Law

Spanish must be covered by a rule with the force of law, which

may establish additional requirements related to your security and

confidentiality.

In particular, said rule may protect the processing of data

in the field of health when required by the management of the systems and

health and social assistance services, public and private, or the execution

of an insurance contract to which the affected party is a party.

Likewise, in relation to the processing of health data, the

LOPDGDD contains specific provisions in its additional provision

seventeenth, stating in section 1 the following:

1. They are covered by letters g), h), i) and j) of the article

9.2 of Regulation (EU) 2016/679 data processing

related to health and genetic data that are regulated in

the following laws and their development provisions:

a) Law 14/1986, of April 25, General Health.

b) Law 31/1995, of November 8, on Risk Prevention

Labor.

c) Law 41/2002, of November 14, basic regulation of the

patient autonomy and rights and obligations in terms of

information and clinical documentation.

d) Law 16/2003, of May 28, on cohesion and quality of

National system of health.

health professions.

e) Law 44/2003, of November 21, on the management of

f) Law 14/2007, of July 3, on Biomedical Research.

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

h) Law 20/2015, of July 14, on management, supervision and

solvency of insurance and reinsurance entities.

i) The consolidated text of the Law on guarantees and rational use of

105 medicines and health products, approved by Royal Decree

Legislative 1/2015, of July 24.

j) The consolidated text of the General Law on the rights of

people with disabilities and their social inclusion, approved by Royal

Legislative Decree 1/2013 of November 29.

However, as indicated in the Report of this Agency 101/2019,

[…] the content of the seventeenth additional provision of the

LOPDGDD must be considered that although a list is established

exhaustive, said circumstance does not prevent the processing of data of

health can rely on other standards that are not cited in the same

provided that any of the circumstances provided for in the

article 9.2 of the RGPD and the regulation established for that purpose has range

law and comply with the guarantees that the Constitutional Court considers

essential when dealing with special categories

of data.

For its part, article 6 of the RGPD establishes the assumptions that

allow the processing of data to be considered lawful, according to which

indicates the following:

1. The treatment will only be lawful if at least one of the

following conditions:

a) the interested party gave his consent for the treatment of his

personal data for one or more specific purposes;

b) the treatment is necessary for the execution of a contract in

which the interested party is a party or for the application at the request of the latter of

pre-contractual measures;

c) the treatment is necessary for the fulfillment of a

legal obligation applicable to the data controller;

d) the processing is necessary to protect the vital interests of the

interested party or another natural person;

e) the treatment is necessary for the fulfillment of a mission

carried out in the public interest or in the exercise of public powers

conferred on the data controller;

f) the treatment is necessary for the satisfaction of interests

legitimate pursued by the data controller or by a

third party, provided that the interests do not prevail over said interests.

or the fundamental rights and freedoms of the interested party that require

the protection of personal data, in particular when the interested party is

child.

Legal cabinet

As has been revealed, articles 6 and 9 of the RGPD

determine the assumptions that allow the processing of personal data, with

general character, and with specific character with respect to the categories

special data, respectively.

For its part, article 8 of the LOPDGDD under the heading “Treatment of

data by legal obligation, public interest or exercise of public powers”

sets the following:

1. The processing of personal data can only be considered

based on compliance with a legal obligation required by the

responsible, in the terms provided in article 6.1.c) of the

Regulation (EU) 2016/679, when so provided for by a regulation of

Law of the European Union or a regulation with the force of law, which may

determine the general conditions of the treatment and the types of data

object of the same as well as the transfers that proceed as

consequence of the fulfillment of the legal obligation. Said rule

may also impose special conditions on the processing, such

such as the adoption of additional security measures or other

established in Chapter IV of Regulation (EU) 2016/679.

2. The processing of personal data can only be considered

based on the fulfillment of a mission carried out in the public interest or

in the exercise of public powers conferred on the controller, in the

terms provided for in article 6.1 e) of Regulation (EU) 2016/679,

when it derives from a competence attributed by a norm with rank

Of law.

Lastly, once the concurrence of any of the

exceptions of article 9.2. and a legal basis of article 6.1., must be given

compliance with the rest of the principles contained in article 5 of the RGPD:

1. The personal data will be:

a) processed lawfully, fairly and transparently in relation to the

interested party (“lawfulness, loyalty and transparency”);

b) collected for specific, explicit and legitimate purposes, and not

will be further processed in a manner incompatible with those purposes;

according to article 89, paragraph 1, the further treatment of the

personal data for archiving purposes in the public interest,

scientific and historical research or statistical purposes shall not be considered

incompatible with the original purposes ("purpose limitation");

c) adequate, pertinent and limited to what is necessary in relation to

for the purposes for which they are processed ("data minimization");

d) accurate and, if necessary, updated; all will be adopted

reasonable measures so that they are deleted or rectified without delay

personal data that is inaccurate with respect to the purposes for

those discussed ("accuracy");

e) maintained in such a way as to allow the identification of the

stakeholders for no longer than is necessary for the purposes of the

processing of personal data; personal data may

be kept for longer periods as long as they are treated

exclusively for archiving purposes in the public interest, purposes of

scientific or historical research or statistical purposes, in accordance

with article 89, paragraph 1, without prejudice to the application of the

appropriate technical and organizational measures imposed by this

Regulation in order to protect the rights and freedoms of the interested party

(“Limitation of retention period”);

f) treated in such a way as to guarantee the safety

adequate use of personal data, including protection against

unauthorized or unlawful treatment and against its loss, destruction or

accidental damage, through the application of technical measures or

appropriate organizational measures ("integrity and confidentiality").

2. The data controller shall be responsible for the

compliance with the provisions of paragraph 1 and able to demonstrate it

("proactive responsibility").

IV

Once exposed, in general, the legal framework applicable to

health treatments, it is appropriate to analyze the possible concurrence of any of the

assumptions that allow lifting the prohibition of data processing of

health in accordance with article 9.2. of the RGPD and article 9.2. of the LOPDGDD and,

particularly, given the competences attributed to the requesting Office, the

provided for in letter g) of article 9.2. of the GDPR:

g) the treatment is necessary for reasons of an essential public interest,

on the basis of the law of the Union or of the Member States, which

must be proportional to the objective pursued, respect essentially the

right to data protection and establish adequate measures and

specific to protect the interests and fundamental rights of the

interested.

In relation to the interpretation and scope of said precept, it has been

recently pronounced by this Agency in its reports 31/2019 and 36/2020:

“However, when dealing with special categories of data, the

assumption referred to in letter g) of article 9.2. does not refer only to

the existence of a public interest, as it does in many other

its precepts the RGPD, but it is the only precept of the RGPD that

requires that it be "essential", an adjective that comes to qualify

this public interest, taking into account the importance and necessity of

greater protection of the processed data.

Said precept finds its precedent in article 8.4 of the Directive

95/46/EC of the European Parliament and of the Council, of October 24,

1995, relative to the protection of natural persons with regard to the

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

"4. Provided they have adequate guarantees, the States
Members may, for reasons of important public interest, establish
other exceptions, in addition to those provided for in section 2, either
through its national legislation, either by decision of the
control". However, its reading results in a greater rigor in the new
regulation by the RGPD, since the adjective "important" is replaced by
“essential” and it is not allowed that the exception can be established by the
control authorities.

In relation to what should be understood as public interest
essential, the jurisprudence of the
European Court of Human Rights, which under article 8
of the European Convention on Human Rights, has been considering that
the processing of personal data constitutes a lawful interference in the
right to respect for private life and can only be carried out if
performs in accordance with the law, serves a legitimate purpose, respects the
essence of fundamental rights and freedoms and it is necessary and
proportionate in a democratic society to achieve an end
legitimate (D.L. against Bulgaria, no. 7472/14, May 19, 2016,
Dragojević v. Croatia, #68955/11, 15 January 2015, Peck
v. United Kingdom, No. 44647/98, January 28, 2003, Leander v.
Sweden, No. 9248/81, March 26, 1987, among others). As he points out in
the last sentence cited, "the concept of necessity implies that the
interference responds to a pressing social need and, in particular,
that it is proportionate to the legitimate aim pursued”.

Likewise, the doctrine of the Court should be taken into account

Constitutional regarding restrictions on the fundamental right to

data protection, which it synthesizes in its sentence 292/2000, of 30

November, in which after configuring the fundamental right to

protection of personal data as an autonomous right and

independent power consisting of a power of disposition and control

on personal data that empowers the person to decide which

of these data provide to a third party, be it the State or an individual, or

which this third party can collect, and which also allows the individual

know who owns that personal data and for what, being able to

oppose that possession or use, analyzes its limits, pointing out

in the following:

More specifically, in the aforementioned Judgments regarding the

data protection, this Court has declared that the right to

data protection is not unlimited, and although the Constitution does not

expressly impose specific limits, or refer to the

Public Powers for its determination as it has done with other

fundamental rights, there is no doubt that they must

find them in the remaining fundamental rights and goods

constitutionally protected legal rights, as required by the

principle of unity of the Constitution (SSTC 11/1981, of 8

April, F. 7; 196/1987, of December 11 [RTC 1987, 196], F. 6; Y

regarding art. 18, the STC 110/1984, F. 5). Those limits or

may be direct restrictions on the fundamental right itself,

which have been alluded to before, or they may be restrictions on the

mode, time or place of exercise of the fundamental right. At

In the first case, regulating these limits is a form of development of the

fundamental right. In the second, the limits that are set

are to the concrete form in which the beam of

powers that make up the content of the fundamental right in

issue, constituting a way to regulate its exercise, which

can be done by the ordinary legislator in accordance with the provisions of the

art. 53.1 CE. The first observation that must be made, which

obviously it is less capital, it is that the Constitution has wanted

that the Law, and only the Law, can set the limits to a right

fundamental. Fundamental rights can yield, from

then, before goods, and even interests constitutionally

relevant, as long as the cut they experience is

necessary to achieve the intended legitimate purpose, proportionate to

achieve it and, in any case, be respectful of the content

essential of the restricted fundamental right (SSTC 57/1994, of

February 28 [RTC 1994, 57], F. 6; 18/1999, of February 22

[RTC 1999, 18], F. 2).

Precisely, if the Law is the only one authorized by the Constitution

to set limits on fundamental rights and, in the case

present, to the fundamental right to data protection, and those

limits cannot be different from those constitutionally

foreseen, which in this case are none other than those derived from the

coexistence of this fundamental right with other rights and
legal goods of constitutional rank, legal empowerment
that allows a Public Power to collect, store, treat, use and,
where appropriate, transferring personal data is only justified if
responds to the protection of other fundamental rights or
constitutionally protected assets. Therefore, if those
Operations with a person's personal data are not
carried out in strict compliance with the rules that regulate it,
violates the right to data protection, since they are imposed
constitutionally illegitimate limits, either to its content or to the
exercise of the bundle of faculties that compose it. as it
will also violate that limiting Law if it regulates the limits of
in such a way as to make the fundamental right impracticable

c. George John 6

28001 Madrid

Legal cabinet

affected or ineffective the guarantee that the Constitution grants. And so
will be when the Law, which must regulate the limits to the rights
principles with scrupulous respect for their essential content,
is limited to empowering another Public Power to set in each case
the restrictions that may be imposed on the rights
fundamental, whose singular determination and application will be at the
albur of the decisions adopted by that Public Power, who
will be able to decide, in what interests us now, on obtaining,

storage, processing, use and transfer of personal data

in the cases it deems convenient and wielding, even,

interests or assets that are not protected with constitutional status

[...]". (Legal Basis 11)

"On the one hand, because although this Court has declared that the

Constitution does not prevent the State from protecting rights or property

legal rights at the cost of the sacrifice of others equally recognized and,

therefore, that the legislator may impose limitations on the

content of fundamental rights or their exercise,

We have also specified that, in such cases, these

limitations must be justified in the protection of other

constitutional rights or assets (SSTC 104/2000, of 13

April [RTC 2000, 104] , F. 8 and those cited there) and, in addition, they must

be proportionate to the purpose pursued with them (SSTC 11/1981, F.

5, and 196/1987, F. 6). For otherwise they would incur the

arbitrariness proscribed by art. 9.3 EC.

On the other hand, even having a constitutional basis and

the limitations of the right being proportionate

established by a Law (STC 178/1985 [RTC

1985, 178]), they can violate the Constitution if they suffer from

lack of certainty and predictability in the very limits they impose

and its mode of application. Conclusion that is corroborated in the

jurisprudence of the European Court of Human Rights that

has been cited in F. 8 and that here must be considered as reproduced. Y

It should also be noted that it would not only harm the principle of

legal certainty (art. 9.3 CE), conceived as certainty about the

applicable law and reasonably founded expectation of

the person on what should be the action of power applying

the Law (STC 104/2000, F. 7, for all), but at the same

time said Law would be injuring the essential content of the

fundamental right thus restricted, given that the way in which it is

have set its limits make it unrecognizable and make it impossible, in the

practice, its exercise (SSTC 11/1981, F. 15; 142/1993, of 22

April [RTC 1993, 142], F. 4, and 341/1993, of November 18

[RTC 1993, 341], F. 7). Luckily, the lack of precision of the

Law in the material assumptions of the limitation of a right

fundamental is likely to generate an indeterminacy about

the cases to which such a restriction applies. And when this occurs

As a result, beyond any reasonable interpretation, the Law no longer

fulfills its function of guaranteeing the fundamental right itself

that it restricts, because it allows instead to operate simply the

will of the person who has to apply it, thus undermining both the

effectiveness of the fundamental right such as legal certainty […]".

(FJ15).

"More specifically, in relation to the fundamental right to

privacy we have emphasized not only the need for

its possible limitations are based on a legal provision

that have constitutional justification and that are proportionate

(SSTC 110/1984, F. 3, and 254/1993, F. 7) but the Law that

restrict this right must accurately state each and every

one of the material budgets of the limiting measure. From

If this is not the case, it is difficult to understand that the judicial decision or the act

administrative authority that applies it are founded on the Law, since

what she has done, abandoning her duties, is

empower other Public Powers so that they are the ones

set the limits to the fundamental right (SSTC 37/1989, of 15

February [RTC 1989, 37], and 49/1999, of April 5 [RTC 1999,

49]).

Similarly, regarding the right to data protection

personal it can be estimated that the constitutional legitimacy of the

restriction of this right cannot be based, by itself, on

the activity of the Public Administration. Nor is it enough that the

Law empowers it to specify in each case its limits,

limiting itself to indicating that it must make such precision when

any constitutionally protected right or asset concurs. Is

the legislator who must determine when that good or

right that justifies the restriction of the right to protection of

personal data and under what circumstances it can be limited and,

furthermore, it is he who must do it by means of precise rules that

make the imposition of such limitation and its consequences foreseeable for the interested party.

consequences. For otherwise the legislator would have moved

to the Administration the performance of a function that only he

competent in terms of fundamental rights by virtue of the

Law reservation of art. 53.1 CE, that is, to clearly establish the

limit and its regulation. […] (FJ 16)".

Likewise, our Constitutional Court has already had the opportunity

to pronounce specifically on article 9.2.g) of the RGPD,

as a result of challenging article 58 bis of the Law

Organic 5/1985, of June 19, of the General Electoral Regime,

introduced by the third final provision of Organic Law 3/2018, of

c. George John 6

28001 Madrid

Legal cabinet

December 5, Protection of Personal Data and guarantee of the

digital rights, regarding the legitimacy of data collection

information relating to the political opinions of the persons who carry

carried out by political parties in the framework of their electoral activities,

precept that was declared unconstitutional by Judgment no.

76/2019 of May 22.

Said sentence analyzes, in the first place, the legal regime

that is subject to the treatment of special categories

of data in the RGPD:

In accordance with section 1 of art. 9 GDPR, it is prohibited to

processing of personal data revealing opinions

policies, in the same way that data processing is

revealing racial or ethnic origin, religious convictions

religious or philosophical beliefs or trade union membership and the treatment of

genetic data, biometric data aimed at identifying

unambiguously to a natural person, data related to health or

data relating to the sexual life or sexual orientation of a

Physical person. However, section 2 of the same precept

authorizes the processing of all such data when it concurs

any of the ten circumstances provided therein [letters a) to j)].

Some of those circumstances have a scope

limited (labour, social, associative, health, judicial, etc.) or

respond to a specific purpose, so that, in themselves,

define the specific treatments that they authorize as

exception to the general rule. Furthermore, the enabling efficacy of

several of the assumptions foreseen there is conditioned to the fact that the

The law of the Union or that of the Member States provides for them and

expressly regulate in their field of competence: this is the case

of the circumstances listed in letters a), b), g), h), i) and j).

Treatment of special categories of personal data

is one of the areas in which expressly the

General Data Protection Regulation has recognized the

Member States "room for manoeuvre" when it comes to "specifying

its standards", as qualified by its recital 10. This

margin of legislative configuration extends both to the

determination of the qualifying causes for treatment

of specially protected personal data - that is, to the

identification of essential public interest purposes and the

assessment of the proportionality of the treatment to the end

persecuted, respecting essentially the right to

data protection - such as the establishment of "measures

adequate and specific to protect the interests and

fundamental rights of the interested party" [art. 9.2 g) RGPD].

Regulation therefore contains a specific obligation to

Member States to establish such guarantees, in the

c. George John 6

28001 Madrid

Legal cabinet

in the event that they authorize the processing of personal data

specially protected.

In relation to the first of the requirements demanded by article

9.2.g), the invocation of an essential public interest and the necessary

specification thereof, the High Court recalls what was stated in its

judgment 292/2000 in which it was rejected that the identification of the

legitimate purposes of the restriction could be carried out through concepts

generic or vague formulas, considering that the restriction of the right

fundamental to the protection of personal data cannot be based,

by itself, in the generic invocation of an indeterminate "interest

public" :

In the aforementioned STC 292/2000 (RTC 2000, 292), in which

legislative interference in the right to

protection of personal data, we reject that the identification

of the legitimate purposes of the restriction could be carried out through

generic concepts or vague formulas:

"16. [...] Similarly, with respect to the right to protection of

personal data it can be estimated that the constitutional legitimacy of

the restriction of this right cannot be based, by itself,

in the activity of the Public Administration. Nor is it enough that the

Law empowers it to specify in each case its limits,

limiting itself to indicating that it must make such precision when

any constitutionally protected right or asset concurs. Is

the legislator who must determine when that good or

right that justifies the restriction of the right to protection of

personal data and under what circumstances it can be limited and,

furthermore, it is he who must do it by means of precise rules that

make the imposition of such limitation and its consequences foreseeable for the interested party.

consequences. For otherwise the legislator would have moved

to the Administration the performance of a function that only he

competent in terms of fundamental rights by virtue of the

Law reservation of art. 53.1 CE, that is, to clearly establish the

limit and its regulation.

17. In the present case, employment by the LOPD (RCL 2018, 1629)

in your art. 24.1 of the expression "control functions and

verification", opens up a space of uncertainty so wide that

provokes a double and perverse consequence. On one side, to

enable the LOPD to the Administration to restrict rights

fundamental principles by invoking such an expression is renouncing

to set the limits itself, empowering the Administration to

do it. And in such a way that, as the Defender of the

Town, allows to redirect to the same practically all

administrative activity, since all administrative activity that

involves establishing a legal relationship with a company, which

This will be the case in practically all cases in which the

c. George John 6

28001 Madrid

Legal cabinet

Administration needs someone's personal data,

will ordinarily entail the power of the Administration of

verify and control that the administrator has acted in accordance with the

administrative legal regime of the legal relationship established

with the Administration. What, in view of the reason for restriction

of the right to be informed of art. 5 LOPD, leave in the most

absolute uncertainty to the citizen about in which cases

that circumstance will occur (if not in all) and add to the

inefficiency any jurisdictional protection mechanism that must

prosecute such a case of restriction of rights

without any other complementary criterion that comes in

help of its control of administrative action in this

matter.

The same reproaches also deserve the use in art. 24.2

LOPD of the expression "public interest" as the basis of the

imposition of limits to the fundamental rights of art. 18.1 and

4 CE, since it contains an even greater degree of uncertainty. Enough

note that all administrative activity, ultimately,

pursues the safeguarding of general interests, whose

achievement constitutes the purpose to which it must serve with

objectivity the Administration in accordance with art. 103.1 CE."

This argument is fully transferable to the present.

prosecution. Likewise, therefore, we must conclude that the

constitutional legitimacy of the restriction of the right

fundamental to the protection of personal data cannot be

based, by itself, on the generic invocation of a

unspecified "public interest". For otherwise the legislator

would have moved the political parties - to whom the provision

challenged authorizes to collect personal data related to the

political views of people within the framework of their

electoral activities - the performance of a function that only

he is responsible for fundamental rights under the

Law reservation of art. 53.1 EC, that is, clearly establish

its limits and regulation.

Nor can we accept, because it is equally imprecise, the purpose

adduced by the State attorney, which refers to the

functioning of the democratic system, since it also contains

a high degree of uncertainty and may involve a

circular reasoning. On the one hand, political parties are

itself "channels necessary for the operation of the system

democratic" (for all, STC 48/2003, of March 12 (RTC

2003, 48), FJ 5); and, on the other hand, the entire operation of the

democratic system ultimately seeks to safeguard

of the purposes, values and constitutional goods, but this does not

manages to identify the reason why the

affected fundamental right.

Finally, it should be specified that it is not necessary to be able to

suspect, with greater or lesser grounds, that the restriction

pursues an unconstitutional purpose, or that the data that is

collect and process will be harmful to the private sphere and the

exercise of the rights of individuals. It is enough with

note that, since it was not possible to identify with sufficient precision

the purpose of the data processing, nor can the

constitutionally legitimate nature of that purpose, nor, in its

case, the proportionality of the planned measure in accordance with

the principles of suitability, necessity and proportionality in

Strict sense.

On the other hand, regarding the guarantees that the

legislator, the aforementioned ruling no. 76/2019 of May 22, after

remember that “In view of the potential intrusive effects on the

affected fundamental right resulting from data processing

personal, the jurisprudence of this Court requires the legislator that,

In addition to meeting the above requirements, you also

establish adequate guarantees of a technical, organizational and

procedural, which prevent risks of different probability and

severity and mitigate its effects, because only in this way can the

respect for the essential content of the fundamental right itself", analyzes

What is the standard that must contain the aforementioned guarantees:

"Therefore, the resolution of this challenge requires that

Let us clarify a doubt that has arisen regarding the scope of our

doctrine of adequate safeguards, which consists of

determine whether adequate safeguards against the use of the

computing must be contained in the law itself that authorizes and

regulates that use or can also be found in other sources

regulations.

The question can only have a constitutional answer. The

Provision of adequate guarantees cannot be deferred to a

time after the legal regulation of data processing

personal in question. Adequate collateral must be

incorporated into the legal regulation of the processing, whether

directly or by express and perfectly delimited reference to

external sources that have the appropriate regulatory status. Only

This understanding is compatible with the double requirement that

stems from art. 53.1 CE (RCL 1978, 2836) for the legislator of

fundamental rights: the reservation of law for regulation

of the exercise of the fundamental rights recognized in the

second chapter of the first title of the Constitution and respect

of the essential content of said fundamental rights.

According to reiterated constitutional doctrine, the reservation of law is not

limits itself to requiring that a law authorizes the restrictive measure of

c. George John 6

28001 Madrid

Legal cabinet

fundamental rights, but it is also necessary, according to

both to demands called -sometimes- of

normative predetermination and -others- of quality of the law as well as

respect for the essential content of the law, which in this regulation

the legislator, who is primarily obliged to weigh the

conflicting rights or interests, predetermine the assumptions, the

conditions and guarantees in which the adoption of

restrictive measures of fundamental rights. That mandate of

predetermination regarding essential elements, linked

also ultimately to the judgment of proportionality of the

limitation of the fundamental right, cannot be deferred to

further legal or regulatory development, nor can it be

leave in the hands of the individuals themselves" (FJ 8).

Therefore, the processing of health data under

of article 9.2.g) requires that it be provided for in a regulation of

European or national law, having in the latter case

said norm, according to the aforementioned constitutional doctrine and the provisions

in article 9.2 of the LOPDGDD, range of law. Said law shall

also specify the essential public interest that justifies the

restriction of the right to protection of personal data and in

what circumstances can be limited, establishing the rules

precise that make foreseeable the imposition of such

limitation and its consequences, without it being sufficient, to these

effects, the generic invocation of a public interest. and said law

It must also establish the appropriate technical guarantees,

organizational and procedural, that prevent the risks of different

likelihood and severity and mitigate their effects.

In addition, said law must respect in all cases the principle

of proportionality, as recalled in the Judgment of the Court

Constitutional 14/2003, of January 28:

In other words, in accordance with a long-standing doctrine of

this Court, the constitutionality of any restrictive measure

of fundamental rights is determined by the strict

observance of the principle of proportionality. For the purposes that

matter here it suffices to remember that, to check whether a

restrictive measure of a fundamental right exceeds the judgment of

proportionality, it is necessary to verify if it meets the three

following requirements or conditions: if the measure is susceptible to

achieve the proposed objective (judgment of suitability); Yes, besides,

is necessary, in the sense that there is no other measure

moderate for the achievement of such purpose with equal effectiveness

(judgment of necessity); and, finally, if it is weighted or

balanced, because it derives more benefits or advantages for

the general interest that harms other goods or values in

conflict (judgment of proportionality in the strict sense; SSTC

66/1995, of May 8 [RTC 1995, 66], F. 5; 55/1996, of 28 of

March [RTC 1996, 55], FF. 7, 8 and 9; 270/1996, dated 16

December [RTC 1996, 270], F. 4.e; 37/1998, of February 17

[RTC 1998, 37], F. 8; 186/2000, of July 10 [RTC 2000, 186]

, F. 6).”

As already indicated, the ECHR considers that the fundamental right

to the protection of personal data is part of the field of

application of the right to respect for private and family life, enshrined in

Article 8 of the ECHR. Section 2 of said precept establishes that “no

There may be interference by the public authority in the exercise of this right.

but insofar as this interference is provided for by law and constitutes a

extent that, in a democratic society, is necessary for the security

security, public safety, the economic well-being of the country, the defense of the

order and the prevention of criminal offences, the protection of health or

of morals, or the protection of the rights and freedoms of others”.

Regarding the processing of personal data for a purpose

different, it must be based on the principle of limitation of the purpose contained in the

article 5.1.b) of the RGPD, according to which personal data will be “collected

for specific, explicit and legitimate purposes, and will not be processed further

in a manner incompatible with said purposes; according to article 89,

section 1, further processing of personal data for archiving purposes

in the public interest, scientific and historical research purposes or

statistics will not be considered incompatible with the initial purposes”.

In relation to the treatment for different purposes, article 6, in its

section 4 states that:

“When the treatment for another purpose other than that for which it is

collected the personal data is not based on the consent of the

interested party or in the Law of the Union or of the Member States that

constitutes a necessary and proportional measure in a society

democracy to safeguard the objectives indicated in article 23,

section 1, the data controller, in order to determine whether the

processing for another purpose is compatible with the purpose for which it was

initially collected the personal data, will take into account, among

other things:

a) any relationship between the purposes for which they were collected

the personal data and the purposes of the intended further processing;

b) the context in which the personal data was collected, in

particular as regards the relationship between the data subjects and the

data controller;

c. George John 6

28001 Madrid

www.aepd.es

26

Legal cabinet

c) the nature of the personal data, specifically when they are processed

special categories of personal data, in accordance with the

article 9, or personal data relating to convictions and offenses

criminal, in accordance with article 10;

d) the possible consequences for the interested parties of the treatment

further anticipated;

e) the existence of adequate safeguards, which may include encryption or

pseudonymization".

In accordance with these precepts, the purpose and legitimate activity of

who processes the data will limit the possibility of collecting and processing the data.

themselves, and must also be limited to the data provided or appropriate to

such purpose. It is not lawful to process data that exceeds what is

necessary for the fulfillment of the objective pursued.

At the same time, the data may only be used for the purposes

that justify this collection and, as we will see, of those who should have been

informed the affected, not being lawful use for other purposes.

And the treatment for different purposes without the consent of the

affected is exceptional, to the point that article 6.4 provides that it may

be established by the law of the Union or of the Member States, provided

that "constitutes a necessary and proportional measure in a society

democracy to safeguard the objectives indicated in article 23.1":

a) State security;

b) defense;

c) public safety;

d) the prevention, investigation, detection or prosecution of

criminal offenses or the execution of criminal sanctions, including the protection

against threats to public security and their prevention;

e) other important objectives of general public interest of the Union or of

a Member State, in particular a significant economic or financial interest

of the Union or of a Member State, including in the tax,

budgetary and monetary, public health and social security;

f) the protection of judicial independence and procedures

judicial;

g) the prevention, investigation, detection and prosecution of

breaches of ethical standards in regulated professions;

h) a related supervisory, inspection or regulatory function,

even occasionally, with the exercise of public authority in cases

referred to in letters a) to e) and g);

i) the protection of the data subject or the rights and freedoms of others;

j) the execution of civil suits".

c. George John 6

28001 Madrid

www.aepd.es

Legal cabinet

Therefore, both by applying Article 9.2.g) and Article 9.2.g)

article 6.4, the proposed data processing requires a standard with a range

of law that enables it.

The ECHR of May 4, 2000 (Case Rotaru v. Romania),

echoing the aforementioned judgment of February 16, 2000, reiterated to his

time for many others (within the most recent one can be mentioned that of 4

December 2015 – Zakharov v. Russia-), recalls that "Both the

storage of such data and its use, together with the refusal to

granting the plaintiff the power to refute them, constitute an interference in

their right to respect for their private life guaranteed by article 8.1". bliss

interference must be respectful of what is established in the aforementioned

article 8.1, recalling the ECHR of February 16, 2000 that "the words

"provided for by law" imply conditions that go beyond the existence of

a legal basis in domestic law and require that it be "accessible" and

"predictable"", which requires analyzing the "quality" of the limiting norm of

right.

This doctrine, collected by our Constitutional Court in the

aforementioned terms, implies that the Enabling Law must

be in force and fulfill the judgment of proportionality, not being enough the

mere formal adoption of the provision to “validate” or “legitimize” without further ado

Treatment of personal data.

v

On the other hand, it should also be taken into account the doctrine

jurisprudence contrary to massive transfers of personal data between

administrative bodies.

In this sense, the interpretation that the Court

Constitutional made of article 16.3 of the Law of Bases of Regime in its

Judgment 17/2013, of January 31, 2013, in which it determined the

constitutionality of it.

As it has been interpreted by the TC in said judgment (FJ 8), this

precept refers to the non-consensual transfer of data related to the

residence or domicile to other public administrations that so request

only in those cases in which, for the exercise of its powers,

be those relevant data. In short, this petition, which does not refer

specifically to the transfer of data from the register with regard to the data

of foreigners, its purpose is to be able to dispose of the data related to the

residence or domicile that appear in the municipal register, (...).

way, in accordance with the Organic Law on data protection, the purpose

that justified the collection of data by an Administration

does not prevent the subsequent destination of the data for its use in purposes

different from those that motivated its collection, respecting, in any case, the

c. George John 6

www.aepd.es

28001 Madrid

28

Legal cabinet

principle of reserve of law to establish said change, (...) the Law of bases

of local regime in its condition, in addition, of regulatory norm of a file

how the municipal register can foresee transfers of data between

Public administrations.

(...) the data transferred must be strictly necessary for the

fulfillment of the functions assigned to the administrative bodies of

form that the request of those data that result

relevant, since it is necessary to distinguish between the analysis and monitoring of a

individualized situation relating to a specific case and the supply

generalized and indiscriminate of all the information contained in a record

personal. The precept has contemplated both extremes in such a way that

any transfer of data from the register must be based on the need

by the assignee Administration acting in the exercise of its

competences, to know, in each specific case, the data related to the domicile

of the affected person, extremes that must be adequately assessed

by the assignor in order to assess whether the data requested is really

necessary, pertinent and proportionate, taking into account the competence that

intends to exercise the assignee Administration (art. 4 in fine of Law 30/1992).

It is thus a rule in itself restricted to data relating to the

residence and domicile in each specific case, and to which they will result from

application, needless to say, the rest of the principles and provisions that

make up the content of the right recognized in the legislation on

Data Protection.

Likewise, the aforementioned ruling of the Constitutional Court 17/2013

analyzed, in its Ninth Legal Basis, a specific assumption of

access to the register data, electronically, by the General Directorate of

the Police, for the exclusive purpose of exercising the powers

established in the Organic Law of Rights and Freedoms of Foreigners

in Spain and its Social Integration, on control and permanence of foreigners

in Spain, and which is included in the seventh additional provision of the LBRL,

introduced by art. 3.5 of Organic Law 14/2003, of November 20, in

which indicates the following:

"Now then, said legal provision must be understood in accordance with

with the requirements of proportionality that our doctrine requires in the

limitation of a fundamental right such as the one concerned here,

regarding the protection of personal data. That means the

transfer of data that the access regulated by the precept supposes must

come surrounded by a series of specific guarantees, guarantees that,

completed by the administrative body to which the precept makes

reference, are obviously susceptible to control. Among them is

finds the need to expressly motivate and justify both the

specific attribution of the condition of user for telematic access

to the data of the register that the precept foresees, such as the specific

accesses in question, avoiding – as long as the required motivation
of such decisions facilitates their corresponding control through the
mechanisms provided for in the legal system, especially through
of the Contentious-Administrative jurisdictional control – that occurs
both a tortious use of said power and indiscriminate access or
massive. Limits to access content that also result from
certain provisions of ordinary legality, which must be
applied bearing in mind, in any case, the necessary unity of the
legal system, such as art. 16.3 LBRL, which we have already
examined or even other specific regulations of the Organic Law
of data protection, especially its art. 22.2. It follows that the
Access will only be possible, under the aforementioned conditions, when
the specific data in question is relevant and necessary in relation to
with the purpose that has justified the access, being guaranteed the
possibility of analyzing whether, in each specific case, the access was protected
in what is established in the Law because, otherwise, it will not be possible
its use. With such guarantees, access regulated in the provision
questioned turns out to be proportionate in relation to the purpose
pursued, since, while the resulting data can only be
used for the purpose established in the precept, must be carried out in
in a timely manner by whoever is expressly authorized to do so
and in relation to specific data whose need must also be
expressly justified and, therefore, subject to control, in the

terms that we have just exposed.

From what was transcribed above, and from the rest of the legal foundation

contained in said sentence, it turns out that the TC has determined that (i) it will have to

avoid indiscriminate and massive access to personal data (ii) the data in

question requested must be pertinent and necessary (iii) for the purpose

established in precept (iv) the request for access to the specific data

must be expressly motivated and justified, (v) so that

this enables its control by the transferor (vi) and avoids a tortious use of that

faculty with massive access. This means (vii) that it must be guaranteed

the possibility of analyzing whether in each specific case the access was protected in terms of

established by law (art. 16.3 LBRL).

In the same sense, the Court of Justice of the Union has ruled

Union, highlighting the existing limits to mass communications of

personal data even in the cases in which they were requested by the

competent authorities for the prevention, investigation, inquiry and

prosecution of crimes.

Indeed, the Court has had the opportunity to rule on the

in accordance with Union law, and in particular with articles 7 and

8 of the Charter of Fundamental Rights of the European Union of a

derivative law of the Union, Directive 2006/24/EC, which allowed

the conservation by the operators of the traffic data generated by the

subscribers and users of electronic communications for their communication to the competent authorities for the detection, prevention, investigation and prosecution of serious crimes, considering that said measure violates said precepts, for which it declares it invalid (judgment of April 8, 2014, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and others).

Subsequently, in his judgment of December 21, 2016 (Affairs C-2013/15 and C-698/15, Tele2 Sverige AB and others) the Court analyzed whether the national regulations transposing the aforementioned Directive 2006/24/CE could be considered in conformity with Union Law, appreciating that there was no such conformity in a rule that provided for the generalized and indiscriminate collection of data and does not subject access to the same to the previous administrative and judicial control.

In relation to the first of the aforementioned questions, the section 94 of the judgment recalled that “according to article 52, section 1, of the Charter, any limitation of the exercise of the rights and freedoms recognized by it must be established by law and respect its content essential”, adding section 96 that “respect for the principle of proportionality is also deduced from the reiterated jurisprudence of the Court of Justice according to which the protection of the fundamental right to respect for private life at Union level requires that exceptions to the protection of personal data and the limitations of that protection exceed what is strictly necessary (judgments of December 16, 2008, Satakunnan Markkinapörssi and Satamedia, C-73/07, EU:C:2008:727, paragraph 56; of November 9, 2010, Volker and Markus Schecke and Eifert, C-92/09 and C-93/09, EU:C:2010:662, paragraph 77; Digital Rights, section 52, and

of October 6, 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 92)".

That said, in accordance with section 100, "the interference that

a regulation of this type in the fundamental rights recognized in the

Articles 7 and 8 of the Charter is of great magnitude and must be considered

especially serious." And section 103 adds that "although it is true that the

effectiveness of the fight against serious crime, especially against

organized crime and terrorism, may depend to a large extent on the

use of modern research techniques, this objective of general interest,

However fundamental it may be, it cannot by itself justify that a regulation

that establishes the generalized and undifferentiated conservation of all

traffic and location data should be considered necessary to the

effects of this fight (see, by analogy, with regard to Directive 2006/24, the

Digital Rights ruling, section 51).

It is thus concluded that "a national regulation such as the controversial one in the

therefore exceeds the limits of what is strictly necessary

and cannot be considered justified in a democratic society, as required

Article 15(1) of Directive 2002/58, in relation to articles

7, 8, 11 and 52, section 1, of the Charter (section 107), being however

in accordance with Union Law "a regulation that allows, on a

preventive, the selective conservation of traffic data and location to

effects of the fight against serious crime, provided that the conservation

of the data is limited to what is strictly necessary in relation to the

categories of data to be kept, the means of communication to which

refer, the affected persons and the established conservation period”

(section 108), for which the national standard "must establish, first of all,

place, clear and precise rules governing the scope and application of a

measure of conservation of data of this type and that establish some

minimum requirements so that the persons whose data have been

conserved have sufficient guarantees to protect from

effectively protect your personal data from the risks of abuse. Should

indicate, in particular, under what circumstances and according to what requirements

preventive measures may be taken to preserve the

data, guaranteeing that such measure is limited to what is strictly necessary

(see, by analogy, with respect to Directive 2006/24, the judgment Digital

Rights, section 54 and cited case law)” (section 109). paragraph 11

points out that the delimitation of the affected group “can be guaranteed through

a geographical criterion when the competent national authorities

consider, on the basis of objective elements, that there is a high risk

preparation or commission of such crimes in one or more areas

geographical”.

For its part, regarding the second of the issues mentioned; this

is, the one related to independent and prior judicial or administrative control, the

The Court states in section 116 that “in relation to respect for the principle

of proportionality, a national regulation that regulates the requirements with

under which communications service providers

electronic networks should grant competent national authorities access

to the conserved data must guarantee, in accordance with what is expressed in the

sections 95 and 96 of this judgment, that such access only occurs

within the limits of what is strictly necessary.

In the opinion of the Court, it will be “national law in which it must determine

the requirements under which service providers

electronic communications must grant such access. However, the

national legislation in question cannot be limited to requiring that access

responds to one of the objectives referred to in article 15, paragraph 1,

of Directive 2002/58, not even the fight against serious crime.

Indeed, such national regulations must also establish the requirements

material and procedural that regulate the access of the authorities

competent national authorities to the retained data (see, by analogy,

with respect to Directive 2006/24, the Digital Rights ruling, paragraph 61)”

(paragraph 118).

Section 120 concludes that “In order to guarantee in practice the full

compliance with these requirements, it is essential that the access of the authorities

competent nationals to the retained data is subject, in principle,

except in duly justified cases of urgency, to a prior control of a

jurisdictional body or an independent administrative entity, and that the

decision of this jurisdictional body or of this entity occurs as a result of

a reasoned request from those authorities, submitted, in particular, in the

framework of prevention procedures, discovery or criminal actions

(see, by analogy, with respect to Directive 2006/24, the judgment Digital

Rights, section 62; see also, by analogy, in connection with the

Article 8 of the ECHR, ECHR, January 12, 2016, Szabó and Vissy v. Hungary,

CE:ECHR:2016:0112JUD003713814, §§ 77 and 80)".

In this way, as has been repeatedly pointed out by this

Agency, the doctrine just revealed requires that the

mass processing of data for the prosecution of crime is delimited

clearly from a triple point of view: on the one hand, data is minimized

object of treatment; on the other, limit the cases in which access to

data can be carried, specifying for example the nature of the crimes

whose seriousness justifies such access; and lastly, that there is a control, that in

the case of Spain should be judicial, prior to effective access to

information.

SAW

Once the regulations and jurisprudence applicable to the

resolution of this consultation, in order to assess the adequacy to the

personal data protection regulations of the information request

carried out by the Office for the Prevention and Fight against Corruption in the Illes

The Balearic Islands should highlight the following:

In the first place, that the aforementioned Office has been created, as indicated

in its Statement of Motives, as a measure to improve quality

democracy and a tool to combat fraud and corruption, and

"Aims to prevent and investigate possible cases of use or destination

fraudulent use of public funds or any illicit use derived

of conduct that entails a conflict of interest or the particular use of

information derived from the functions of the personnel at the service of the

public sector". Likewise, it adds that “The creation of this office fulfills the

provided for in article 6 of the United Nations Convention against

corruption, approved in New York on October 31, 2003, for the fact

that guarantees the existence of a specialized and independent body

responsible for preventing corruption.

The aforementioned United Nations Convention against Corruption,

ratified on June 9, 2006 and in force for Spain since July 19,

c. George John 6

2006, highlights in its Preamble the concern for "the seriousness of the

problems and threats posed by corruption to the stability and

security of societies by undermining the institutions and values of the

democracy, ethics and justice and by compromising sustainable development and

rule of law".

Likewise, the fight against corruption is included in other

European standards, such as the Convention on combating acts of

corruption involving Community officials

European Union or of the Member States of the European Union, done in Brussels

on May 26, 1997, or in other more recent ones such as the latest Directives

on public procurement, incorporated into our legal system by the

Law 9/2017, of November 8, on Public Sector Contracts, which establishes

Transpose to the Spanish legal system the Directives of the Parliament

European and Council 2014/23/EU and 2014/24/EU, of February 26, 2014.

Therefore, the fight against corruption can be considered,

effects of article 9.2.g) of the RGPD, as an essential public interest.

On the other hand, based on the duty to provide information that imposes

Article 10 of Law 16/2016, of December 9, creating the Office of

Prevention and Fight against Corruption in the Balearic Islands, it provides

a series of guarantees, highlighting the duty of secrecy contained in the article

7.3: “The people who carry out their activity in the Office of Prevention and

Fight against Corruption are obliged to keep secret everything that

know by reason of their function in the legally established terms,

duty that lasts after his cessation in the exercise of the position. Failure to

this duty of secrecy gives rise to the responsibility that, in each case,

appropriate”. Likewise, another guarantee would be those provided for in the article itself.

10.1, when it provides that "access to information must be justified, it is

It must motivate the relationship with the investigated activity and it must be left

proof of this in the file”.

However, while the above circumstances could lead to

consider admissible, in a specific and duly justified case, the access

to certain health data, in the present case, said request is

considered excessive and contrary to data protection regulations

personal, for the following reasons:

First of all, nothing is indicated in the information request

regarding the specific purpose for which the information is claimed, although

attending to it, it seems that it is referred to verifying compliance with the

vaccination protocols for people who have received the vaccine.

And article 9.2.g) of the RGPD requires that the treatment be necessary, and it is not

has justified in the request the need to access the data

personal information of persons vaccinated in connection with the research

is carrying out, which would require carrying out the triple judgment of suitability,

3. 4

Legal cabinet

necessity and proportionality, assessing whether data communication

related to the health of certain persons is necessary for the

compliance with the purpose of controlling the administrative action pursued, and

if said purpose cannot be achieved by other means that do not require the

communication of said data, such as, for example, the communication

of the aggregated information (that is, anonymized, in a way that does not allow the

identification of natural persons) referring to the different vaccination groups

foreseen in the vaccination protocols or not belonging to any of the

them, indicating the total number of people who would be in each

of those assumptions.

On the other hand, because said requirement supposes a massive treatment

of personal data that, as indicated in the query, would affect, at least,

108,500 people, which is contrary to the principle of data minimization and

the doctrine of the Constitutional Court and the Court of Justice of the Union

aforementioned European.

Madrid, May 04, 2021

c. George John 6

28001 Madrid

www.aepd.es