Legal cabinet

N/REF: 0097/2020

Examined your request for a report, forwarded to this Legal Office,
regarding the Draft Order of the Minister of Economic Affairs and
Digital Transformation on non-face-to-face identification methods for
issuance of qualified electronic certificates, requested, as a
urgency, of this Spanish Data Protection Agency in accordance
with the provisions of articles 57.1.c) of 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 data processing
personal information and the free circulation of these data by which the
Directive 95/46/EC (General Data Protection Regulation, RGPD) and 5 b)
of the Statute of the Agency, approved by Royal Decree 428/1993, of 26
March, please let me inform you of the following:

I

As stated in its article 1, the draft order sent
Its purpose is to regulate the conditions and minimum technical requirements
applicable to verification of identity and, if applicable, other attributes
specific, of the applicant for a qualified certificate, through
other methods of identification other than physical presence that provide a
equivalent safety in terms of reliability, in accordance with the provisions of
Article 7.2 of Law 6/2020, of November 11, regulating
certain aspects of electronic trust services and in the
Article 24.1 d) of Regulation (EU) 910/2014, of the European Parliament and of the
Council, of July 23, 2014, regarding electronic identification and
trust services for electronic transactions in the market

interior and repealing Directive 1999/93/EC”.

Said order is issued pursuant to the provisions of article 24.1 of the

Regulation (EU) No. 910/2014, of the European Parliament and of the Council, of 23

of July 2014, regarding electronic identification and identification services

confidence for electronic transactions in the internal market and by the

repealing Directive 1999/93/EC:

Article 24

Requirements for qualified trust service providers

1. When issuing a qualified certificate for a trusted service, a

qualified provider of trust services will verify, by the means

appropriate and in accordance with national law, identity and, if

c. George John 6

28001 Madrid

proceeds, any specific attribute of the natural or legal person to whom

that a qualified certificate is issued.

The information referred to in the first paragraph will be verified by the

trusted service provider either directly or through

of a third party in accordance with national law:

a) in the presence of the natural person or an authorized representative of

the legal person, or

b) remotely, using means of electronic identification, for

which the presence of the natural person or of a

authorized representative of the legal entity prior to the

issuance of the qualified certificate, and that they meet the requirements

established with article 8 with respect to security levels

“substantial” or “high”, or

c) by means of a certificate of a qualified electronic signature or

a qualified electronic seal issued in accordance with letter a) or

b), or

d) using other widely recognized identification methods

that provide equivalent security in terms of reliability

to physical presence. Equivalent security will be confirmed by a

conformity assessment body.

Likewise, it is based on the provision contained in section 2 of the

Article 7 of Law 6/2020, of November 11, regulating certain

aspects of electronic trust services, which by regulating the

Verification of the identity and other circumstances of applicants for a

qualified certificate, provides the following:

2. By regulation, by order of the holder of the

Ministry of Economic Affairs and Digital Transformation,

will determine other conditions and technical requirements for verification of the

remote identity and, if applicable, other attributes specific to the

applicant for a qualified certificate, by other methods

of identification such as videoconference or video-identification that

provide security equivalent in terms of reliability to the

physical presence as assessed by a safety assessment body

conformity. The determination of said conditions and requirements

technicians will be carried out based on the standards that, where appropriate, have

determined at the community level.

Scale-recognized identification methods will be considered

national, for the purposes of the provisions of this section, those

that provide security equivalent in terms of reliability to the

physical presence and whose equivalence in the level of security is

certified by a conformity assessment body,

in accordance with the provisions of the regulations on services

trusted electronics.

c. George John 6

28001 Madrid

On the other hand, as antecedents of said regulation, it manifests itself in

the preamble that “The health emergency generated by the COVID-19 crisis

19 has demanded during the state of alarm the confinement of citizens and

the drastic limitation of personal travel, with a view to curbing the

infection growth. Temporary and exceptional, through the

Eleventh additional provision of Royal Decree-Law 11/2020, of March 31,

by which urgent complementary measures are adopted in the social field and

to deal with COVID-19, a temporary system of

remote identification to obtain qualified certificates, in order to

contribute to reducing the displacement of citizens to carry out

procedures, without undermining their rights. The text of the aforementioned provision, which

was informed by this Agency, is as follows.

Eleventh additional provision. Provisional measures for

issuance of qualified electronic certificates.

During the validity of the state of alarm, decreed by Royal Decree
463/2020, of March 14, the issuance of certificates will be allowed
Qualified electronic devices in accordance with the provisions of article 24.1.d)
of Regulation (EU) 910/2014, of July 23, regarding the identification
electronic and trust services for transactions
electronics in the internal market. To this end, the supervisory body
will accept those methods of identification by videoconference
based on the procedures authorized by the Executive Service of
the Commission for the Prevention of Money Laundering and Offenses
Monetary or recognized for the issuance of qualified certificates
by another Member State of the European Union. The equivalence in
level of security will be certified by an evaluation body of the
accordance. The certificates thus issued will be revoked by the
service provider at the end of the state of alarm, and its use will be
shall be limited exclusively to the relations between the owner and the
Public administrations.
Likewise, it should be cited as background information, although it is not done
reference in the submitted documentation, the fifth additional provision of the
Royal Decree-Law 28/2020, of September 22, on remote work, which does not
contained in the text sent to the report of this Agency, and which modified the Law
of electronic signature with the same purpose intended by article 7.2 of the
Law 6/2020, which has repealed it:
Fifth final provision. Modification of Law 59/2003, of 19
December, electronic signature.
A new section 6 is added to article 13 of Law 59/2003, of 19
December, electronic signature, with the following tenor:

«6. By Order of the person in charge of the Ministry of Economic Affairs and Digital Transformation will determine the conditions and requirements techniques applicable to identity verification and, if applicable, other specific attributes of the person requesting a certificate qualified, through other methods of identification that provide a security equivalent in terms of reliability to physical presence.”

This text corresponds to the one contained in article 7.2. of text of the "Draft Bill on certain aspects of services electronic trust" that was reported by this Agency on February 7 of 2018 (Report 283/2017), with the only difference being the elevation of the range of the provision that should be approved:

“By resolution of the Secretary of State for the Society of the Information and the Digital Agenda will determine the conditions and requirements applicable to verification of identity and, if applicable, other specific attributes of the person requesting a certificate qualified by other means of identification that provide a security equivalent in terms of reliability to physical presence”.

However, the final text of Law 6/2020, following the precedent of Royal Decree Law 11/2020, proceeds to identify some of the means through which such identification may be made, when referring to expressly to the videoconference or video-identification, thus converting

some systems that had been admitted in our legal system

legal with a specific purpose aimed at the prevention of money laundering

capitals for the authorization of face-to-face identification procedures

via videoconference on February 12, 2016 and the authorization of

video-identification procedures of May 11, 2017 of the Service

Executive of the Commission for the Prevention of Money Laundering and

Monetary Offenses (SEPBLAC), and that had been established with

temporary for the issuance of qualified electronic certificates during the

validity of the state of alarm declared as a consequence of the emergency

generated by the COVID-19 crisis, in permanent media

admitted by the legal system to verify identity remotely and

that will not be limited exclusively to service providers

trustworthy electronic devices, since, as the Analysis Report points out

Regulations (MAIN), "these products are very attractive for other types of

companies that need to reliably identify their customers".

On the other hand, the absence of references in the text sent to the

personal data protection regulations, notwithstanding the incidence that the

same has in the subject matter of regulation, insofar as it implies treatment

automated personal data that, in addition, may imply a high

risk to the rights and freedoms of those affected, without being considered

sufficient, for these purposes, the specific references contained in the

Article 9 regarding the adoption of “appropriate measures to guarantee the privacy of the entire identification process of the applicant”, in article 6 regarding the training of the operator in charge of verifying the identity in terms of personal data protection or in article 8 to the refer to remote work.

The need to respect, in any case, the regulations on protection of personal data is expressly collected in the eIDAS Regulation, although referring to the regulations in force at the time of its approval, indicating in its Recital 11 that “This Regulation must be applied in such a way that data protection principles are fully complied with personal data established in Directive 95/46/CE of the European Parliament and of the Tip. To this end, given the principle of mutual recognition that establishes this Regulation, authentication for the purposes of an online service must involve exclusively the processing of identifying data that is adequate, pertinent and not excessive for granting access to the service online in question. On the other hand, service providers confidence and the supervisory body must also respect the requirements of confidentiality and security of the treatment provided for in Directive 95/46/ CE” and establishing in its article 5.1 that “The processing of data will be in accordance with the provisions of Directive 95/46/EC” and containing numerous references to this regulation throughout its articulate. In this same sense, article 8 of Law 6/2020 refers to the personal data protection:

1. The processing of personal data required by providers of trustworthy electronic services for the development of your activity and the administrative bodies for the exercise of the functions attributed

by this Law shall be subject to the provisions of the applicable legislation in

matter of protection of personal data.

2. Trusted electronic service providers that record

a pseudonym in an electronic certificate must verify the

true identity of the certificate holder and retain the

supporting documentation.

3. These trust service providers will be obliged to

reveal the aforementioned identity when requested by the judicial bodies and

other public authorities in the exercise of functions legally

attributed, subject to the provisions of the applicable legislation in

matter of personal data protection.

Therefore, being said regulations applicable to

Processing of personal data necessary for identification

physical persons for the issuance of electronic certificates

that regulates the standard object of the report, you must enter a

Legal cabinet

reference to its observance in the preamble, as well as an article

specific, proposing the following wording:

Article XX. Personal data protection:

“The processing of personal data of natural persons

will be carried out strictly subject to the provisions of the Regulation (EU)

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

on the protection of natural persons with regard to

treatment of your personal data and the free circulation of these

data and in the rest of the regulations on data protection

personal".

However, the mere inclusion of said precept is not considered

sufficient for the purpose of adequately guaranteeing the fundamental right to

the protection of personal data, taking into account the principle of

proactive liability introduced by the General Protection Regulation

of data (GDPR) and the constitutional doctrine regarding the limitations of the

fundamental right to data protection, as analyzed below.

continuation.

II

At the present time, in terms of data protection

personal concerns, the regulations to which the preliminary project must comply

submitted for consultation is Regulation (EU) 2016/679, already cited (GDPR) and the

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

guarantee of digital rights (LOPDGDD).

In this regard, it must be taken into account that the RGPD has meant a

paradigm shift when addressing the regulation of the right to protection of

personal data, which is based on the principle of "accountability"

or "proactive responsibility" as the AEPD has repeatedly pointed out

(Report 17/2019, among many others) and is included in the Explanatory Memorandum

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

Personal and guarantee of digital rights (LOPDGDD): "the greatest

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

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

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". Inside this new

system, it is the data controller who, through the instruments

regulated in the RGPD itself, such as the registration of treatment activities, the

risk analysis or data protection impact assessment

Legal cabinet

personal, must guarantee the protection of said right through the

compliance with all the principles contained in article 5.1 of the RGPD,

adequately documenting all the decisions it adopts for the purpose of

be able to prove it.

Likewise, based on said principle of proactive responsibility,

essentially addressed to the data controller, and in order to reinforce the

protection of those affected, the RGPD has introduced new obligations

required not only to the person in charge, but in certain cases, also to the

in charge of the treatment, who may be sanctioned in case of

non-compliance with them.

Therefore, being the main recipients of the obligations

collected in the RGPD those responsible and in charge, however, their

observance implies the need to adopt certain behaviors by

part of the national legislator, in order to guarantee compliance with the GDPR

and, ultimately, the adoption of sufficient guarantees for the protection of the

fundamental right, especially when it comes to data processing

legitimized personal as a result of the fulfillment of obligations

legal or for the fulfillment of a mission of public interest or the exercise of

public powers.

In this regard, it should be remembered, as indicated in our

Report 283/2017, that the processing of personal data necessary to

verify the identity and circumstances of the certificate applicants

will be legitimized by article 6.1 c) of the General Regulations of

Data Protection, which enables treatment based on a legal obligation

imposed by domestic or European Union law.

In these cases, the RGPD contains specific provisions to the

respect, starting with those provided for in its own article 6, paragraphs 2 and

3:

2. Member States may maintain or introduce provisions

more specific in order to adapt the application of the rules of the

this Regulation with respect to the treatment in compliance with the

section 1, letters c) and e), establishing more precise requirements

specific treatment and other measures that guarantee a

lawful and equitable treatment, including other situations

specific treatment under chapter IX.

3. The basis of the treatment indicated in section 1, letters c) and e),

must be established by:

a) Union law, or

b) the law of the Member States that applies to the

responsible for the treatment.

The purpose of the treatment must be determined on said basis.

legal or, in relation to the treatment referred to in section 1, letter

c. George John 6

28001 Madrid

e), will be necessary for the fulfillment of a mission carried out in

public interest or in the exercise of public powers vested in the

responsible for the treatment. Said legal basis may contain

specific provisions to adapt the application of rules of the

this Regulation, among others: the general conditions that govern the

legality of the treatment by the person in charge; object data types

of treatment; affected stakeholders; the entities to which

may communicate personal data and the purposes of such communication; the

purpose limitation; the terms of conservation of the data, as well

such as operations and treatment procedures, including

measures to ensure fair and lawful treatment, such as

relating to other specific situations of treatment under the

chapter IX. The law of the Union or of the Member States shall comply

an objective of public interest and will be proportional to the legitimate purpose

pursued.

Likewise, article 4, after defining in section 7 the

“responsible for the treatment” or “responsible” as “the natural person or

legal entity, public authority, service or other body which, alone or jointly with others,

determine the purposes and means of the treatment” adds that “if the Law of the

Union or of the Member States determines the purposes and means of the treatment,

the data controller or the specific criteria for their appointment

may be established by the Law of the Union or of the Member States".

On the other hand, article 35 regulates the impact assessment related to the

data protection (EIPD), noting that "When it is likely that a type

of treatment, in particular if it uses new technologies, by its nature,

scope, context or purposes, entails a high risk for the rights and freedoms

of natural persons, the person in charge of the treatment will carry out, before the

processing, an assessment of the impact of processing operations on

the protection of personal data. A single evaluation may address a

series of similar processing operations involving high risks

Similar". However, said precept provides that the EIPD has been carried out

previously by the legislator in section 10:

10. When the treatment in accordance with article 6, paragraph 1,

letters c) or e), has its legal basis in the Law of the Union or in the

Law of the Member State that applies to the person responsible for the

treatment, such Law regulates the specific operation of treatment or

set of operations in question, and a

impact assessment relating to data protection as part of

an overall impact assessment in the context of the adoption of

said legal basis, sections 1 to 7 will not apply except if

Member States consider it necessary to carry out such an assessment

prior to treatment activities.

On the other hand, it should also be taken into account that, in the event that the obligation is imposed by a rule of domestic law, the same must have the status of law, as required by article 53.1 of the Constitution, as as expressly stated in article 8.1 of the LOPDGDD, adding that "will be able to 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. This rule may also impose special conditions to the treatment, such as the adoption of additional security measures or others established in the Chapter IV of Regulation (EU) 2016/679" and the constitutional doctrine collected, fundamentally, in the judgments 292/2000 of November 30 and 76/2019 of May 22, according to which the Limits to the fundamental right to the protection of personal data must be be established by a standard with the force of law, prior weighting by the legislator of the interests in conflict according to the principle of proportionality, defining each and every one of the material budgets of the limiting measure by means of precise rules, which make the concerned the imposition of such limitation and its consequences, and establishing adequate guarantees, being the law itself the one that will have to contain the adequate guarantees against the collection of personal data that you authorize. The Constitutional Court (TC) has been clear that the forecast of the adequate guarantees cannot be deferred to a time after the legal regulation of the processing of personal data in question. The Adequate guarantees must be incorporated into the legal regulation of the

treatment, either directly or by express referral and perfectly

limited to external sources that have the appropriate regulatory status. Only

that understanding is compatible with the double requirement that stems from the

article 53.1 EC (...). It is evident that, if the rule included a reference to

the integration of the law with the adequate guarantees established in rules of

lower rank than the law, it would be considered as a delegalization that

sacrifices the reserve of law ex article 53.1 CE, and, for this reason alone, it should

be declared unconstitutional and invalid. (...). It is, in short, about “guarantees

adequate technical, organizational and procedural nature, which prevent

risks of different probability and severity and mitigate their effects, since only

In this way, respect for the essential content of the right itself can be ensured.

fundamental". Nor does it serve for this reason that for the establishment of said

adequate and specific guarantees the law refers to the RGPD itself or to the

LOPDGDD.

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

proportionality, as recalled by the ruling of the Constitutional Court

14/2003, of January 28:

In other words, in accordance with a settled 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, enough

to remember that, in order to check whether a restrictive measure of a fundamental right exceeds the judgment of proportionality, it is necessary verify if it meets the following three requirements or conditions: if the measure is capable of achieving the proposed objective (judgment of suitability); if, in addition, it is necessary, in the sense that there is no other more moderate measure to achieve such purpose with equal effectiveness (judgment of necessity); and, finally, if it is weighted or balanced, because more benefits or advantages are derived from it for the general interest that harms other goods or values in conflict (judgment of proportionality in the strict sense; SSTC 66/1995, of 8 May [RTC 1995, 66], F. 5; 55/1996, of March 28 [RTC 1996, 55] , FF. 7, 8 and 9; 270/1996, of December 16 [RTC 1996, 270], F. 4.e; 37/1998, of February 17 [RTC 1998, 37], F. 8; 186/2000, of 10 of July [RTC 2000, 186], F. 6).”

The same doctrine maintains the Court of Justice of the European Union (CJEU). Thus, if art. 8 of the European Charter of Fundamental Rights recognizes the right of every person to the protection of personal data personnel that concern him, art. 52.1 recognizes that this right is not unlimited and allows the limitation of the exercise of those rights and freedoms recognized by the Charter, a limitation that must be established by law and respect their essential content.

Well, the STJUE of October 6, 2020, in the accumulated cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net and others, (not available still to this date in Spanish), in section 175, recalls that:

With regard to the justification for such interference, the requirement, established in Article 52(1) of the Charter, that any limitation on the

exercise of fundamental rights must be provided for by law implies that the legal basis which permits that interference with those rights must itself defines the scope of the limitation on the exercise of the right concerned (see, to that effect, judgment of 16 July 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 175 and the case-law cited).

Likewise, section 65 of the Judgment (STJUE) of the same date 6 October 2020 (C-623/17), Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and others, citing, as above, the Schrems 2 sentence, says:

It should be added that the requirement that any limitation on the exercise of fundamental rights should be established by law implies that the legal basis that allows the interference in said rights must define it

same the scope of the limitation of the exercise of the right that try (judgment of July 16, 2020, Facebook Ireland and Schrems, C-311/18, EU:C:2020:559, paragraph 175 and cited case law).

In short, section 175 of the STJUE of July 16, 2020, C-311/2020, Schrems 2, says: It should be added, on this last aspect, that the requirement that any limitation on the exercise of rights must be established by law implies that the legal basis that allows interference in said rights, it must itself define the scope of

the limitation of the exercise of the right in question [opinion 1/15 (Agreement EU-Canada PNR), dated July 26, 2017, EU:C:2017:592, paragraph 139 and case law cited].

It is therefore the same law that establishes the interference in the right the fundamental one that has to determine the conditions and guarantees, that is, the scope and limitation, which must be observed in said treatments,

And in said STJUE of July 16, 2020, Schrems 2, it is added (and subsequently reiterates in the aforementioned judgments of October 6, 2020):

176 Finally, to meet the proportionality requirement under the which exceptions to the protection of personal data and the limitations of that protection must not exceed what is strictly necessary, the controversial legislation that entails the interference must establish clear and precise rules governing the scope and application of the measure in question and impose certain requirements minimum, so that the persons whose data have been transferred have sufficient guarantees to protect effective your personal data against the risks of abuse. In particular, said regulations must indicate in what circumstances and with Under what requirements can a measure be adopted that provides for the processing of such data, thus guaranteeing that the interference is limited to what is strictly necessary. The need to have such guarantees is of particular importance when the personal data is subjected to automated processing [see, in this regard, opinion 1/15 (EU-Canada PNR Agreement), July 26, 2017, EU:C:2017:592, sections 140 and 141 and cited case law).

The STJUE of October 6, 2020, in case C-623/17, adds the

mention of special categories of data:

68 (…) These considerations are applicable in particular when it is

at stake the protection of that particular category of data

personal data that are sensitive data [see, in this sense, the

judgments of April 8, 2014, Digital Rights Ireland and others, C-293/12

and C-594/12, EU:C:2014:238, sections 54 and 55, and of December 21,

c. George John 6

28001 Madrid

eleven

Legal cabinet

2016, Tele2, C-203/15 and C-698/15, EU:C:2016:970, paragraph 117;

Opinion 1/15 (EU-Canada PNR Agreement), of July 26, 2017,

EU:C:2017:592, paragraph 141].

Based on the regulations and the cited jurisprudential doctrine, this

The Agency has been pointing out in its most recent reports the need for,

by the legislator, by introducing regulations in our legal system

legal that have special importance in the data processing of

personal character, proceed previously to an analysis of the risks that

may derive from them, including in the Analysis Report of

Normative Impact a systematized study of the impact that in the right

fundamental to the protection of personal data of the interested parties must

have the different data treatments provided by law. In this sense it

have pronounced Report 77/2020, regarding the Draft Organic Law

Fight against Doping in Sport or Report 74/2020 referring to the

Preliminary project of the Law of democratic memory.

Applying these criteria to the present case, we must start from the basis

that the informed norm would lack, according to the jurisprudence

cited so far, of the appropriate range to establish limitations to the

fundamental right to data protection, being the regulation

contained in article 7 of Law 6/2020, which has introduced the possibility

that verification of identity is carried out by other means of

identification such as videoconference or video-identification, enabling the

regulatory development to determine the conditions and technical requirements

thereof, which may not affect the fundamental right to protection

of data. Therefore, it is considered essential, given the purpose of the

norm object of the report, that the incidence that

the same may have in the processing of personal data, for the purpose

to avoid any excess of the same that would be determinant of

its nullity.

implement

Also, claiming the rule that organizational measures and

procedures that must

providers are

proportionate to the risks and appropriate to the nature of these services

with respect to some certificates that, in the words of its preamble “constitute

an authentic digital alter ego of the person”, and adding the MAIN, among its

specific objectives, that of "providing citizens with an alternative

safe from the legal and technical point of view to the physical person for the

obtaining qualified certificates”, and also considering that it has

positive effect on innovation, since “it will allow the development and implementation

in the market for innovative and safe technological solutions”,

the detailed analysis of the risks that it may have for the rights and

freedoms of citizens will allow the measures that are

c. George John 6

28001 Madrid

www.aepd.es

established in the order also respond to the necessary security

of personal data.

For these reasons, it is considered necessary to assess the impact that

the regulation contained has in the fundamental right to protection

of data, to guarantee the adequate protection of the fundamental right

to the data protection of the interested parties, being desirable in these

assumptions a greater dialogue with this Agency, similar to the one

has maintained with the National Cryptologic Center, the sector of

trusted service providers and solutions manufacturers

remote identification.

III

Analyzing the articulated text from the perspective of protection

of personal data, it is interesting to highlight the following:

In the first place, the legality of the treatment of the character data

personnel will require the existence of a legal basis that legitimizes the

treatment, taking into account that the RGPD, unlike what

occurred in the previous regulations, has placed all the legal bases standing

of equality, so that consent is collected as one of the six

causes of legitimation for the treatment without showing greater or lesser

importance than the rest regulating, even, assumptions in which the

The consent of the affected party should not constitute the legal basis of the treatment.

As the AEPD has been pointing out since its report 65/2017, the RGPD has

displaced the "principle of consent" as the central axis of the right to

data protection, so "it can no longer be said that there is

exceptions to consent, but, since consent is one of the

possible legitimate bases of the treatment will not proceed to collect it in the

assumptions in which the treatment is covered by any of the

the remaining causes causes included in article 6.1 of the general regulation

of data protection".

In the present case, the legal basis that legitimizes the treatment, as

As stated above, it is the one provided for in letter c) of article 6.

of the RGPD (the treatment is necessary for the fulfillment of an obligation

law applicable to the data controller), so, for these purposes, we do not

The consent of the affected party must be obtained.

However, in the event that the possible personal data to be processed by the

providers (since they will have to verify the identity, or, if applicable, other

specific attributes of the applicant for a qualified certificate, art.

7.2 law 6/2020) in the case of any of the special categories of data to

those referred to in article 9.1. of the RGPD will be necessary, in advance,

that any of the causes that lift the prohibition of its

treatment, in accordance with article 9.2. of the RGPD and article 9 of the LOPDGDD.

For these purposes, the order refers to its article 9.8. to the "comparison

biometric performed", which could involve data processing

biometrics aimed at the unique identification of the person. To this

In this regard, there is no legal norm that protects said treatment by the

existence of an essential public interest, with the requirements and guarantees

mentioned above, said treatment could only be based on what

provided for in letter a) of article 9.2. of the RGPD: "the interested party gave his

explicit consent for the processing of said personal data with

one or more of the specified purposes, except when Union Law or

of the Member States establishes that the prohibition mentioned in the

section 1 cannot be raised by the interested party", not finding the

treatment of said biometric data between the cases in which the article

9.1 of the LOPDGDD provides that the sole consent of the affected party does not

suffice to lift the ban on data processing. However, the

consent must comply, in any case, with the requirements contained in

the RGPD itself, which defines consent in its article 4.11 as "all

manifestation of free, specific, informed and unequivocal will by which

the interested party accepts, either by means of a declaration or a clear action

affirmative, the treatment of personal data that concerns you",

requiring, in addition, in this case, as indicated in article 9.2.a) that the

itself be explicit. Also, special consideration should be given, as

as indicated in our report 36/2020, that consent must be

free, pointing out Recital 42 of the RGPD that "Consent must not

be considered freely provided when the interested party does not enjoy true or

free choice or you cannot withhold or withdraw your consent without prejudice

any", for which reason, in any case, other forms of

identification through the use of other technologies, which do not require the

processing of biometric data, in order to guarantee freedom of choice

of the affected.

For all these reasons, article 9.2., relative to the conditions

of the identification process, which provides that "The

express consent of the applicant, including consent to the

full recording of the identification process", since said

consent, from a data protection perspective

personal, it would only be necessary in the case of the treatment of

special categories of personal data, and must then be provided

in a differentiated manner with respect to any other consent that is

deemed necessary, in accordance with article 7.2. of the RGPD, and must,

likewise, guarantee other alternative forms of identification that do not

entail such reinforced interference in the fundamental right to

protection of personal data that implies the recording and conservation

your image and your biometric data. And, in the event that it is intended

impose as an obligation for non-face-to-face identification the

processing of biometric data aimed at the unique identification of

the person, said obligation would require its establishment by a norm

with the force of law, attending to an essential public interest, which establishes

the appropriate guarantees, in accordance with article 9.2.g) of the RGPD: “the

processing is necessary for reasons of 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 and specific measures to

protect the interests and fundamental rights of the interested party”

IV

Second, once the above requirements have been met, they must

Take all appropriate measures to ensure compliance with the

principles that are included in article 5 of the RGPD, in addition to the principle of

aforementioned legality:

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 will not be

further processed in a manner incompatible with those purposes; from

according to article 89, paragraph 1, further processing of data

for archival purposes in the public interest, research purposes

scientific and historical or statistical purposes shall not be considered incompatible

for the original purposes (“purpose limitation”);

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

purposes for which they are processed (“data minimization”);

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

reasonable measures to promptly remove or rectify the

personal data that is inaccurate with respect to the purposes for which

that are treated ("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) processed in such a way as to ensure adequate security of

personal data, including protection against unlawful processing

authorized or unlawful and against loss, destruction or accidental damage,

through the application of appropriate technical or organizational measures

("integrity and confidentiality").

2. The data controller will be responsible for compliance with

the provisions of section 1 and capable of demonstrating it ("responsibility

proactive").

For these purposes, it must be included, within the information to which

refers to article 9 of the order, in its section 1 ("The

applicant, in a clear and understandable manner, of the terms and

conditions of the process of remote identification by video, as well as of

the applicable safety recommendations") that provided for in the

personal data protection regulations, in the terms indicated

in article 13 of the RGPD, being able to provide said information "by

layers", under article 11 of the LOPDGDD.

Likewise, special attention must be paid to the principles of limitation

of the purpose and minimization of data as manifestations of the principle

of proportionality, analyzing whether the data to be processed are strictly the

necessary for the intended purpose and if there are no other alternatives

Less burdensome personal data processing for the affected party. TO

these effects, it must be assumed that the order develops article 7.2 of the Law

6/2020, as expressly stated in its article 1, which refers to other

identification methods other than physical presence, among which he cites the

videoconference or video-identification but without excluding others, while the

order is limited exclusively to them, so the first thing that

should be assessed is whether there are also no other alternative means,

that may even be less invasive, such as through

remote verification of the information contained in the certificate itself

of the DNI or identification by a trusted third party.

On the other hand, within the modalities of remote identification by

video, article 3 of the order states that "The process of remote identification

by video can be carried out in an assisted manner, with the synchronous mediation of a

operator, or unassisted, without the need for online interaction between a

operator and the applicant, with subsequent review by an operator. Therefore, it

admits a non-assisted modality, much more invasive and that will

necessarily require the recording of the images (as

generally established in article 11 of the order), which would require

a specific assessment regarding, in the first place, the need for said

treatment from the point of view of its proportionality, and in the case

that it is deemed necessary, the adoption of reinforced guarantees

from the point of view of personal data protection.

Likewise, by virtue of the principle of proactive responsibility, when

regulate in article 5 the general safety requirements should be included

expressly the need to carry out the risk analysis for the

rights and freedoms of natural persons required by article 24 of the

RGPD, in accordance with the principles of privacy by default and from the

design contemplated in article 25 of the RGPD and the need to carry out

an EIPD in accordance with article 35, expressly providing that, in

measures to be implemented as a result of the aforementioned risk analysis

shall prevail over any other. Also, these measures should

be reviewed and updated as necessary, which will occur not only in

in the event of changes to the system, as provided for in the

article 5.1. of the order, but at any time when you have

knowledge that they are not adequate or are not sufficient,

as it can be when there is knowledge of vulnerabilities that

may give rise to security breaches and for which there is no solution

at that time, or due to changes in the context, the procedures

organizational or technological advances. For that very reason,
reference should be made to the establishment of privacy audits and
continuous review of privacy measures aimed at improvement
continuous compliance with regulations regarding data protection and the
implementation of the necessary corrective measures to improve safety
of personal data. Ultimately, it is about adopting a model of
continuous risk management, as advanced by this Agency in the
Practical Guide for Risk Analysis in the Processing of Personal Data
subject to the RGPD:
Given the constant technological evolution and the processes of
digital transformation suffered by data processing activities
personal data, it is crucial to address these processes from a model
focused on continuous risk management, defining from the design
the necessary control and security measures so that the treatment
born respecting the privacy requirements associated with the level of
risk to which it is exposed and periodically evaluating the
effectiveness of the control measures implemented.
On the other hand, section 6 of the aforementioned
Article 5, in order to collect the obligation to notify breaches of
security that affect personal data to this Agency without delay
undue, in the terms provided in article 33 of the RGPD.
Likewise, by regulating article 8 the requirements of the facilities,
the possible location of the servers should be assessed, to the extent
that may entail the existence of international transfers of
data, which would require, therefore, that they comply with the
requirements established in Chapter V of the RGPD, taking into account the

limitations that derive from the interpretation made by the Court of

Justice of the European Union in its recent judgment of July 16, 2020 in

case C-311/18 (Schrems Judgment2), which declares contrary to Law the

Legal cabinet

Decision 2016/1250 of the European Commission referring to transfers to

United States (Privacy Shield).

Regarding the requirements for verifying the identity of the

applicant and the identity document, section 4 establishes the measures

mandatory that must be implemented to detect a possible manipulation of

the video image, of the identity document or of the applicant, among which

there is an obligation to have the affected person with a mobile device

(the risks that this implies for their rights and interests must be assessed)

carry out said treatment compulsorily through a mobile device,

adopting the appropriate guarantees) in which a code must be entered

unique, and the provider must verify "that the mobile device to which it is

sends the code is in the possession of the user" adding that "The

supervisory body may make a platform available to providers

technological verification of the association of the user with the device

mobile".

The aforementioned precept raises a series of questions from the

of view of the protection of personal data, in addition to the outlined

regarding the incidence of having to compulsorily carry out the

treatment through a mobile device, which would require including the

vulnerabilities introduced by the mobile in risk management and EIPD

timely: on the one hand, as the platform is optional, it must be valued and

analyze how else this obligation can be fulfilled

of verification, in order to propose the appropriate guarantees. And on the other,

The database that associates the user with the

mobile device, and its legal basis must be determined by a standard

with the appropriate range and in accordance with the principles of protection of

data, containing neither the text of the order nor the MAIN major

references regarding this platform.

On the other hand, taking into account the principle of data accuracy,

admit article 10.3 that, due to technical problems unrelated to the provider,

can carry out the query that it establishes, can continue with the

identification process “leaving a written record of the incident”,

must be completed in order to establish the obligation to carry out said

consultation as soon as possible, before proceeding to the issuance of the

certificate.

v

For all the reasons stated in the previous sections,

considers it necessary to review the text submitted in order to guarantee

compliance with personal data protection regulations,

assessing all the risks that the approval of the standard can

assume for the rights and freedoms of those affected, for the full

effectiveness of the provisions of the RGPD and the LOPDGDD in accordance with the jurisprudential criteria cited in this report.

For these purposes, it should be noted that data processing that may be currently being carried out for the Non-face-to-face identification of people require, in accordance with the principle of proactive responsibility, that the respective managers have adopted and documented all the necessary measures to guarantee the compliance with the personal data protection regulations, through the timely risk analysis, EIPD, etc., identifying the legal bases that legitimize the treatment and adopting all the necessary guarantees in accordance with the principle of data protection by default and from the design, being, therefore, any breach of said regulations of its exclusive responsibility.

However, at the moment in which one proceeds by a norm law to regulate said treatments, they will be obliged to apply this rule, so it will be necessary to determine previously that it is in accordance with data protection regulations personal. This is especially relevant if, as in the present case, more invasive treatments are protected, such as the identification of unassisted, and specific treatment obligations are established, as the obligation to record in full and in any case the process of identification or, very especially, when affecting special categories of data, the obligation to carry out a biometric comparison, as provides for article 9.8.

For all these reasons, as pointed out at the beginning of this report,

considers it essential to carry out a detailed analysis and

detailed description of the implications that the approval of the standard has for

the rights and freedoms of those affected, in the terms provided in the

RGPD and that have been pointed out throughout this report, of the

as completely as possible within the urgency with which it has been

requested, taking into account that said analysis is of special relevance since

that this order does not attend exclusively to the temporary situation

derived from the Covid-19 pandemic, but rather intends to regulate these

identification processes permanently, to eliminate, in words

of its MAIN “the competitive disadvantage -derived from this regulatory loophole- of

trust service providers established in Spain with respect to

providers established in other EU Member States”.

This analysis will allow to correctly identify all the measures

and guarantees that must be adopted and, especially, those measures

contemplated in the order that, not having a mere technical nature but

regulate treatments that may interfere with the right

fundamental to the protection of personal data, would require a

norm with the rank of law, such as those previously referred to the recording

full identification process, in any case, and data processing

biometrics aimed at the unique identification of the person.

For the reasons stated, an unfavorable report is issued,

pending correction of the observations made.