 Procedure No.: PS/00418/2019

RESOLUTION OF PUNISHMENT PROCEDURE

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

to the following

BACKGROUND

FIRST: Dated 10/30/2018, sent by the Basque Data Protection Agency,

Two claims made by A.A.A., B.B.B.,

C.C.C. and D.D.D. (hereinafter, the claimants) against the entity ZIURTAPEN ETA ZERBITZU

COMPANY-CERTIFICATION AND SERVICES COMPANY IZENPE, S.A.,

with NIF

A01337260 (hereinafter IZENPE or the claimed party), in relation to the process of collecting

biometric data of Basque citizens, particularly users of the Service

Vasco de Empleo LANBIDE, supported by communications posted on bulletin boards

of the offices of this entity with the following text:

“Soon it will be necessary to digitally identify Lanbide users.

For this reason, we invite you to stop by the collection post once your attention is over.

biometric data”.

The complainants consider that, if the collection of data is established as mandatory

to formalize certain procedures, consent would not be free. They understand that

violates the provisions of Recital 60 of Regulation (EU) 2016/679, which requires the

responsible for providing the interested party with as much information as “necessary to guarantee a

fair and transparent treatment” and to “inform the interested parties if they are obliged to provide the

data and the consequences in the event that they do not do so”; and Considering 43 of the same

Regulation, according to which “to ensure that consent has been freely given,

this should not constitute a valid legal basis for the processing of the data in a

specific case in which there is a clear imbalance between the interested party and the person responsible for the treatment, in particular when the controller is a public authority.

They add that opinion 3/2012, on the evolution of biometric technologies, of the Working Group of Article 29, has already warned that in order to consider freely granted the consent there must be a valid alternative to identification.

They provide a copy of the collaboration agreement signed by LANBIDE and IZENPE for the implementation of electronic means of identification based on data capture biometrics, of October 26, 2017 (published on 03/26/2018), which regulates the deployment of means of electronic identification of natural persons, based on data collection biometrics As stated in the agreement, the content of which is outlined in Fact Proven Third, LANBIDE will act as IZENPE's registration entity for the issuance means of digital identification and electronic signature. Likewise, it is specified that IZENPE (trust service provider) will be responsible for the files that process the data and that LANBIDE acts as data processor.

As a result of these claims, which were initially filed with the Basque Data Protection Agency, this entity, on 07/06/2018, carried out inspection in one of LANBIDE's dependencies. In the document prepared by this action, which is provided by one of the claimants, the acting inspection indicated the Next:

. The fingerprint collection process was verified, which entails the treatment of the DNI/NIE/Passport; collection of the fingerprints of the ten fingers of the hands and the facial image.

. The representatives of the entity stated that ten operational positions were arranged

for the pilot fingerprint collection experience, having collected 5,900 to date

biometric data of job seekers and income guarantee income. The

collection is voluntary.

The forecast is to expand the collection in the 43 Lanbide offices at the end of 2018.

. LANBIDE does not use biometric data to identify users as they are not

system operational. These data are stored by IZENPE

. It incorporates the informative brochure displayed on the board, the detail of which has already been outlined, the

informative clause that is delivered in the offices and the form for exercising the right

of cancellation (the content of this informative clause is outlined in the Fact

Tested Fifth).

The Basque Agency for Data Protection inadmissible the claims through

resolution of 10/29/2018, also provided by one of the claimants, in which

also agrees to transfer them to this Agency. Consider the Basque Agency for

Data Protection that LANBIDE acts only as a registration entity, being the entity

responsible for data collection IZENPE (public company constituted by the Government

the Basque Country and the Provincial Councils), over which said Agency does not have powers,

be a commercial company not contemplated in the Basque Data Protection Law.

SECOND: The claims outlined were transferred to IZENPE which, on the date

12/05/2018, reported the following:

1.- In 2002, the General Administration of the Autonomous Community of Euskadi and the

Provincial Councils, through their respective public limited companies

information technology, formed the IZENPE company for the development of the identification

electronics.

It is considered a Trust Service Provider according to Regulation (EU) No.

910/2014, that is, entity providing trust services: electronic identification,

electronic signature, etc

IZENPE is part of the Basque public sector and has the status of its own medium

personified by Eusko Jaurlaritzaren Informatika Elkartea - Computer Society of the

Basque Government, S.A. (Ejie), Lantik, S.A., Informatika Zerbitzuen Foru Elkartea - Company

Foral de Servicios Informático S.A. (IZFE) and the Álava Computing Center, S.A. (CCASE)

as determined in Law 9/2017, of November 8, on Public Sector Contracts, by

which the Directives of the European Parliament are transposed into the Spanish legal system

and of the Council 2014/23/UE and 2014/24/UE, of February 26, 2014.

According to the bylaws of the company, provided by IZENPE with its response, the assignments that

carried out by the contracting authorities of which IZENPE is its own medium: (i) they will have

instrumental and non-contractual nature, so for all purposes, they are

internal, dependent and subordinate; (ii) will be articulated through assignments, which will specify the

object, terms and other conditions of the assignment; (iii) they will be mandatory; (iv) it

they will pay through rates set by the body entrusted to you; and (v) will carry the

authority for the body that confers the order to dictate the necessary instructions for its

execution.

It constitutes its object:

a) The promotion of electronic relationships on telecommunications networks, with the

necessary security guarantees.

b) The provision, within the scope of the institutions that make up the Basque public sector, of

security services, technical and organizational, in communications through techniques and

electronic, computer and telematic means.

c) The issuance and management of means and electronic identification systems for the identification, authentication, signature and/or electronic sealing, to persons or public entities or private.

d) Consulting services and any other related to the previous paragraphs.

2.- Since 2016, in its capacity as a medium of the Administrations that participate in its capital, and by order of the same, and within the framework of Regulation (EU) No. 910/2014, IZENPE has been developing the identification media issuance project with centralized certificate (in the cloud) for individuals named B@k and B@KQ.

It seeks to provide citizens with a means of identification, always voluntary, easy to use in telematic relations with the Basque Administrations according to the requirements of each procedure and/or service.

. B@K is defined as a means of low-level electronic identification, made up of a reference number matching the DNI/NIE/Passport of the user and a password; and an unqualified certificate issued in a centralized repository that It will be used for signing acts.

. B@K Q is defined as a mid-level electronic identification medium, consisting of by a reference number that matches the DNI/NIE/Passport of the user and a password; a set of coordinates with 16 positions; and a qualified certificate of electronic signature issued in a centralized repository of IZENPE that will serve for signing acts.

Furthermore, in order to respond to new needs associated with identification, IZENPE has completed the means B@K and B@KQ with other factors of biometric authentication such as fingerprint and/or photograph.

IZENPE states that the order for the provision of various services related to the identification and electronic signature is made to IZENPE, as its own means, through

Resolution (provides a copy) of the Director of Services of the Department of Public Governance and Self-government, which is responsible for the effective implementation in the administrations of the electronic Administration in the administrative procedures and in the management of public affairs, as well as the declaration and management of the common services of electronic processing of the Public Administration of the Autonomous Community of Euskadi.

This resolution states that the assignment constitutes the essential activity of IZENPE, according to its statutes, and are mandatory for this company.

Among other electronic services, the purpose of the assignment is the Integrated Key System eIDAS and includes the creation, verification and validation of identification keys and their preservation.

The supervision of the correct provision of the service corresponds to the Directorate of Attention to Citizenship and Innovation and Improvement of the Administration.

In relation to these orders, IZENPE warns that the one corresponding to the year 2018 will be is pending signature.

3. For its part, LANBIDE, created by Law 3/2011, of October 13, is an organization self-employed of an administrative nature attached to the Department of Employment and Social Policies of the Basque Government, endowed with its own legal personality and full capacity to act to the fulfillment of its purposes, which is entrusted, among other functions, with the management of the intermediation and the execution of active employment policies within the scope jurisdiction of Euskadi, as well as, the management of the economic benefits of guarantee of income in the terms established in Law 18/2008, of December 23, for the Guarantee

Income and for Social Inclusion.

At the end of 2017, based on the volume of applications managed by the body and due to the high number of people attending its offices, the Basque Government and the Department of Employment and Social Policies in the framework of the reform process and modernization of LANBIDE and in order to provide a better service to citizens, decided to implement experimentally in the Autonomous Community of Euskadi, a system identification and electronic recognition through biometric factors (fingerprint and facial features) for all workers and users of the service, in order to improve, simplify and make administrative management more efficient, thus responding to the current needs of society.

He adds that the project is committed to enabling a digital, simple, fast and secure system of identification and authentication of the interested parties in the administrative procedure adjusted to the legal provisions of the LPACAP, and the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, regarding the protection of data of natural persons with regard to the processing of personal data and the free circulation of these data (hereinafter, RGPD), being fully guaranteed the citizenship rights. In addition, the project contributes to consolidate the administration and advance in the digitization of the internal functioning of the Administration.

The system deployment process begins with the prior registration of the parameters chosen biometrics.

In this context, and to promote the deployment and implementation of the digital footprint as means of identification in LANBIDE, this entity and IZENPE signed an agreement of collaboration, of 10/26/2017 (published on 03/26/2018), for the launch of media of electronic identification based on the collection of biometric data, which has been recently extended and modified to adapt it to the new regulatory framework regarding of data protection established after the entry into force, on May 25, 2018, of the

RGPD, through the addendum signed on October 15, 2018, in which the

seventh clause, regarding data protection. In its new wording it is specified that

LANBIDE may not use the data for its own purposes, which will treat them in accordance with the

determined by IZENPE.

After signing the Collaboration Agreement and in its capacity as Registration Entity, LANBIDE

makes its physical spaces available to IZENPE, as well as the personnel in charge of the

user identification and registration tasks, which is duly formed by the latter,

carrying out the following actions:

Verification of your identity.

Capture fingerprints.

Taking a photograph of the face.

Obtain the signature of the request for issuance from B@k and B@kQ.

Register/record the biometric data obtained (photograph and fingerprint) in the system of

IZENPE identity management.

In this regard, IZENPE states that participation in this process is totally

voluntary for users, who are duly informed about the processing of data and

its purpose in accordance with the provisions of article 13 of the RGPD, obtaining its

explicit consent (article 7 RGPD).

LANBIDE has a network of 43 offices distributed throughout the territory of the Community

Autonomous of Euskadi. Project planning to provide means of

Electronic identification with biometric factors to citizens contemplates three phases:

. In a first phase, a biometric data collection station was installed in one of the

LANBIDE offices, on an experimental basis.

. In a second phase, corresponding to the current state and continuing with the

experimental, the deployment has been extended to 10 registration posts, located in paths

Offices.

. In a third phase (to be executed in the second quarter of 2019) it is planned to extend the

number of registration posts to all LANBIDE offices and, in addition,

intends that this means of identification can be used by people who

voluntarily choose it, for access to the services of this entity.

In the first instance, the target public for the use of this identification system is the

formed by the group of users of the Basque Employment Service: applicants

of employment in general, participants in training actions and guidance services, as well as

as applicants for social benefits of the Income Guarantee Income (RGI) and

the Complementary Housing Benefit (PCV). It is a group close to the

300,000 people.

The deployment of the project has been accompanied by communication messages that have been

displayed on informative posters (provides photography) in the offices of LANBIDE. The

exposed information, which did not establish the obligatory nature of its use to access the

services provided by the body, was modified last July. The text of this

poster is as follows:

“In this office a biometric data collection station has been installed for the

digital identification of LANBIDE users.

If you are interested, we invite you to go through booth nº… to obtain the information

that you need and, where appropriate, carry out the necessary procedures”.

The IZENPE entity indicates that, until November 2018, approximately 9,000 people have

requested this means of identification with biometric factors and that, at this time, 3 people have exercised the right to revoke the consent granted.

4. In parallel, in accordance with the regulation on this matter established in the RGPD (which gives biometric data the character of sensitive data and whose legitimizing basis must be be established by Law), the Basque Government has promoted a reform of Law 3/2011, October 13, creation of Lanbide-Basque Employment Service, currently in process, that incorporates into the legal text the use of biometric systems for the identification of users of its services and/or beneficiaries of its benefits.

Until the use of this identification system is regulated by law, it is only being tested experimentally, being necessary to test its operation and continue with the development of the technological tool that supports it.

To this end, by Resolution of the General Director of LANBIDE dated November 30, 2018, it is agreed to “Entrust the company Ziurtapen eta Zerbitzu Enpresa-Empresa de Certification and Services, Izenpe, S.A., as the Administration's own personified means General of the Autonomous Community of Euskadi, the provision of services for the implementation in Lanbide of a system that allows the identification of people based on biometric factors.

As indicated in this resolution, the services object of the order will be carried out in various phases and includes the implementation of a computer solution for the request for means of identification B@k and B@Kq with biometric factors, providing a system management of registration of biometric factors of citizen identification based on facial recognition and fingerprint consisting of the registration and consultation of data from

ID.

The sixth section of this resolution, dedicated to data protection, states that the

The applicable regime will be the one provided for in the RGPD, which IZENPE is responsible for processing,

which is identified in your treatment record with the following detail:

. Treatment: management of means of identification based on biometric parameters.

. Data object of treatment: identification, special categories of data: data

biometrics

. Conservation period: 7/15 years, depending on the means of identification

qualified/qualified, from the formalization of the application.

The order begins its validity on 01/01/2018 and extends until 12/31/2019.

5. IZENPE formulates a series of considerations in relation to what was stated by the

claimants, of which the following should be highlighted:

. IZENPE's interest in completing the means of identification with biometric factors

derives from the impulse carried out by the Basque Government and the Department of Employment and Policies

Social to implement new citizen identification technologies, and

specifically the current order on the need to carry out this adaptation to

meet the management needs of LANBIDE.

. It should be clarified that it is LANBIDE, and not IZENPE, who establishes the purpose of the use of

these means of identification in the provision of its services.

. The issuance of the means B@k and B@kQ is voluntary and they are only issued when

previously the applicant has completed and signed the corresponding request for

issue.

. A specific “frequently asked questions” type document has been prepared for the project

of Lanbide clarifying aspects related to rights and associated risks, as well as on

the circumstances of the use of these means of identification (copy attached).

. IZENPE has the Impact Assessment Report corresponding to the treatment of

data entailed by this identification system with biometric factors. this report

concludes that this system does not pose a significant risk to the privacy of users.

interested. Attached to your letter is the Impact Assessment Report of 07/10/2018 and a

November 2018 update.

. IZENPE has reviewed and clarified the information given to date on the characteristics

of the environment, adapting it to the requirements of the RGPD, and have adapted to the RGPD the

application forms for means of identification B@k and B@kQ with biometric factors (the

content of these new versions is outlined in the Fifth Proven Fact).

THIRD: The claims to which the proceedings refer were admitted to

process through resolutions dated 01/09/2019.

FOURTH: In view of the facts denounced in the claim and the documents

provided by the claimants and IZENPE, the Subdirectorate General for Data Inspection

proceeded to carry out preliminary investigation actions to clarify the

the facts in question, by virtue of the powers of investigation granted to the authorities

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

Data Protection, hereinafter RGPD), and in accordance with the provisions of Title VII,

Chapter I, Second Section, of Organic Law 3/2018, of December 5, on the Protection of

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

Within the framework of these previous actions, the acting inspection requested

information to IZENPE which, on 02/18/2019, submitted the following response:

1. The issuance of the means of electronic identification is carried out as determined in the

document called “Citizen certificate policy”, published at www.izenpe.eus

and notified to the Ministry of Industry, Tourism and Commerce (provides a copy of this document).

It is a document that details and completes what is generically defined in the

IZENPE Certification Practices Statement, www.izenpe.eus/dpc and that describes the

electronic means of identification issued by this company to citizens, in what

here comes the means B@k and B@kQ and defines their life cycle (verification of identity

of the applicant, application procedure, issuance and delivery, as well as the revocation and

renewal).

All stages of the life cycle of a means of identification, except the revocation of a

medium for technical reasons, require the applicant to complete and sign the

corresponding application form. Through the application form you will be informed about

the characteristics of the requested electronic means, conditions of use and applicable legislation

regarding personal data; and personal data is collected from the interested party

necessary for the issuance of the means of identification and your free consent, through

the signature of it.

2. The number of users from whom biometric data has been taken before the

modification of the application forms is 10,378 records, of which 3,624 are

prior to the date of entry into force of the GDPR. After the modification of the forms of

request, 320 registrations have been made until 02/15/2019. The total number of records to said

date amounts, therefore, to 10,738 users.

IZENPE warns that the initial forms were used from 10/26/2017 and that these

were modified on 12/04/2018, although, due to a technical incident, the
new models have not been used until February 5, 2019 (both forms are
contributed with their letter of 05/12/2018).

Provide a copy of these forms. The new application model that, according to IZENPE, is
prepared in December 2018, coincides with the one outlined in the Second Antecedent.

The form that they claim to have used initially and that they provide with this letter of
02/18/2019 contains the following information:

It is reported that the electronic identification, B@k is formed by a reference number
matching the DNI/NIE of the user and a password assigned by IIZENPE; a
non-qualified certificate issued in a centralized repository that will serve for the acts of
signature; and biometric data (fingerprint and photograph). The medium B@kQ is formed,
in addition, by a set of coordinates with 16 positions and a qualified signature certificate
issued in a secure centralized repository of IZENPE, the "cloud", which will serve
for signing acts.

The detail of the data collected and the basic data protection information coincides with
the one outlined in the Fifth Proven Fact.

On the other hand, the form provided has a space enabled for the signature of the
applicant and then a section on “Issue and Activation” is added with the text
following: “After identifying and signing the application form, the applicant may initiate the
issuance of B@k. The process begins with the sending of an SMS with the password (which by
security must change). Lastly, Izenpe will generate a non-qualified signature certificate
electronically issued in a secure centralized repository”.

In the case of B@kQ, another section is included, on the identification of the applicant (of
face-to-face, remotely using means of electronic identification other than the
certificate, certificate of qualified electronic signature or other means) and the documentation of
identification provided or that authorizes to consult, depending on whether the interested party is a Spanish citizen,

EU/EEA member citizen or non-EU citizen.

3. The only treatment that is carried out on said data, as with those obtained with

subsequent to the modification, is derived from the "management of means of identification

based on biometric parameters", whose purpose is the registration of applications and the issuance

of these means of identification, and where appropriate the revocation, as a provider of

trust services.

In the future, the administrations of the Autonomous Community will be able to use the

as means of identification in the management of the identification of citizens.

4. In response to the query that was made about whether they have established a procedure

to review the consents obtained before the modification of the forms of

request, state that all requests have required the interested party to complete

the form and consent to the processing of your data by signing it, and that

has offered the information regarding the characteristics of the medium and its conditions of use,

therefore, they have not considered it necessary to obtain new consents.

FIFTH: On 11/04/2019, a new document from the entity entered this Agency

IZENPE, in which it states that it has carried out an exhaustive analysis of the regulations

applicable to its activity, and, in relation to the processing of biometric data, it indicates the

Next:

. The "Collaboration Agreement" signed with LANBIDE was formulated in accordance with the

data protection regulations prior to the full applicability of the GDPR.

. That once Law 9/2017, of November 8, on public sector contracts, was approved,

IZENPE came to be considered the personified medium of a series of

Basque territorial administrations, specifically the General Administration of

Euskadi, on which LANBIDE depends, as stated in the modification of the statutes of the

merchant that contributes.

. Once the statutes were modified, LANBIDE issued a resolution on 11/30/2018, prior to the

entry into force of the LOPDGDD, which included the condition of own media

personified IZENPE, although the scheme based on the

LOPD of 1999.

. As a consequence of the above, the study carried out recommends the reformulation of the

roles as responsible and in charge of data processing, taking into account the

condition of IZENPE as the medium of its parent administrations.

It adds that at the time the treatment was carried out, the

LOPDGDD and the requirement that the processing of biometric data require a

express recognition in a norm with the force of law, when said treatment was

carried out by the Public Administrations.

Likewise, it warns that, as a conclusion of the aforementioned analysis, and considering that

From the entry into force of the LOPDGDD any data processing by the

public authorities (even more so those whose purpose is the collection of biometric data,

either directly or in its capacity as a personified medium; that is, through

commissions) that is based on reasons of public interest or in the exercise of powers

public requires its coverage or provision by a rule with the force of law; and since, in the

Currently, there is no regulation in the Basque legal system with the rank of Law that

expressly provides for the possibility of carrying out the analyzed treatment based on

reasons of public interest or in the exercise of public powers, as a measure of prudence,

IZENPE has informed LANBIDE of the decision to provisionally suspend the treatment

of the registration of biometric data for the issuance of means of identification to citizens

as long as there is no such legal coverage. Therefore, from October 26, 2019 this

data processing is not being carried out.

The implementation of this identification system is a possibility that is foreseen

expressly in the proposed Law for the Income Guarantee and for the inclusion,

currently in process, which will presumably give legal coverage to LANBIDE, in the

terms established by article 8.2 of the LOPDGDD, to carry out the identification

of citizenship through biometric systems, which could put an end to doubts

reasonable that are presented in the current processing of personal data.

Based on this, and taking into account that IZENPE cannot be sanctioned by a

data processing carried out in its capacity as its own personified medium that acts

through commissions, request the file of the proceedings. It also considers that said

file considering that when the processing of biometric data began it was not

legally defined that the consent of the affected party was not a sufficient legitimate basis for

such treatment.

SIXTH: On 12/18/2019, the Director of the Spanish Data Protection Agency

agreed to initiate a sanctioning procedure against the entity IZENPE, in accordance with the provisions

in article 58.2 of the RGPD, for the alleged infringement of article 4 of the LOPD and article 5

of the RGPD, determining that the sanction that could correspond would be a warning,

without prejudice to what results from the instruction.

Likewise, for the purposes set forth in article 49 of the LOPD and article 58.2.d) of the

RGPD, in said initial agreement the aforementioned entity was warned that the infractions

imputed, if confirmed, may lead to the adoption of the necessary measures to

adapt to the personal data protection regulations the treatment operations that

performs, the information offered to its clients and the procedure by which they

give their consent for the collection and processing of their personal data, with the

scope expressed in the Legal Basis of the repeated agreement and without prejudice to what

resulting from the instruction.

SEVENTH: Having been notified of the aforementioned initiation agreement, IZENPE submitted a brief of allegations in

who requests that a resolution be issued by which the file of the procedure is agreed, of

according to the following considerations:

I.- From the formal point of view, he indicates that he is not aware of any investigative action

specific, beyond giving notice to that party to formulate allegations in relation

with the previous actions that have determined the opening of the procedure; neither

he is aware of no notification from the AEPD indicating the date on which the

the period of preliminary investigation actions, for which it is complex to determine the

compliance with the twelve-month requirements established in article 67.2 of the

LOPDGDD; nor does it have a formal record of the claims that were admitted for processing,

the exact terms in which they were formulated and if they reproduce what was stated before the

Basque Data Protection Agency.

In this section, IZENPE requests a copy of the claims and previous actions of

investigation, reserving the right to formulate additional allegations.

II.- Considers it opportune to specify the temporary space on which the

claims made and its regulatory framework, to correctly delimit the

responsibilities and define the role of IZENPE, in its capacity as responsible for the

treatment or, where appropriate, in charge of the treatment, and define if its action is formal and

instrumental or it is a substantive action resulting from the exercise of one's own

competition. To this end, perform the following time sequence of events:

a) The Lanbide/Izenpe Collaboration Agreement, of October 26, 2017 (published in March 2018), whose sole purpose was the configuration of LANBIDE as a registration entity, was dictates being directly applicable the LOPD and the Basque Parliament Law 2/2004, of files personal and AVPD creation. In that agreement, in accordance with article 12 of the then current LOPD, IZENPE acquires the status of responsible for files, which does not should be confused with the condition of data controller, according to the RGPD.

b) After the entry into force, on 03/08/2018, of Law 9/2017, of November 8, on Contracts of the Public Sector (hereinafter, LCSP), the IZENPE Statutes were adapted and its consideration as the personified means of the General Administration of the Autonomous Community and its public bodies (as is the case of LANBIDE), of in accordance with the provisions of article 32 of the aforementioned Law. However, until then, the mercantile company already had the condition of its own means and technical service, since the modification of its Articles of Association in 2010. And, consequently, it acted materially through encomiendas formalized by the parent entities, among they LANBIDE.

c) When the AVPD Inspection Act is issued on July 6, 2018, as consequence of the complaints filed in relation to the biometric tests carried out, the LCSP was in force and the RGPD was already fully applicable, which was giving its first steps with many unknowns about its scope; but these are events prior to the requirement of a rule with the force of law to have a legitimate basis for treatment by missions carried out in the public interest or in the exercise of public powers (article 8 of the

LOPDGDD). In that Act the following is verified: 1) the Agreement of

collaboration and the distribution of roles collected there; 2) it is not defined which entity fulfills the role of

responsible for the treatment and which one is in charge according to the RGPD; 3) starts from the criterion of

consent as the legitimate basis of the treatment (article 6 RGPD); and 4) it is concluded that

There may have been an infringement of the formalized data protection regulations

through the GDPR.

In addition, IZENPE highlights that when the identification system was launched (October

2017) the RGPD was not yet fully effective, so biometric tests are not

were considered special data. This occurred as a result of the full

GDPR applicability.

d) On October 26, 2018, the extension and modification of the Agreement of

collaboration signed the previous year. The LOPD is still in force in everything that does not

would have been displaced by the GDPR, which was fully applicable. I also know

had approved Royal Decree-Law 5/2018, whose transitory provision referred to the

managers' contracts and their applicability until 2022.

e) Resolution R18-071 of the AVPD inadmits the complaints, in accordance with the provisions of the

Law 2/2004 of the Basque Parliament, which does not attribute powers to that entity to initiate a

disciplinary proceedings against a publicly owned commercial company.

f) On 11/30/2018, within the framework of the RGPD and the LCSP, by Resolution of the

General Management of LANBIDE formalizes the order to IZENPE of "the provision of

identification services based on biometric factors", in its capacity as its own medium

personified of the Basque Government and, specifically, of LANBIDE. This Resolution follows

impregnated, in part, with the reiterated collaboration agreement, since it is characterized

IZENPE as data controller, but its third clause makes it explicit that the

supervision of the correct performance of the assignment belongs to LANBIDE, and is indicated in the clause

second, that it corresponds to this autonomous body to define the purposes of the

treatment.

IZENPE considers that the personified medium itself to which the assignment is made (still

in the case of a registration entity) can not be in any way responsible for the

treatment, given that this instrumental entity does not have the material competence that

force it.

g) From that date, IZENPE, taking into account the file followed in the AEPD,

then in the phase of preliminary actions, and the doubts that the configuration had raised

of the model of actions that had existed until then, chose to propose the non-

renewal of the extension, stop the treatment until there is a legitimate basis

through a Coverage Law (which is being processed in the Basque Parliament) and give

transfer to the AEPD of such extremes by letter of 04/11/2019, to the effect that no

carry out the initiation of the sanctioning file, taking into account its consideration of

instrumental entity as a personified means of its own that did not define the ends or the objective

of the treatment. Given this condition, IZENPE could not effectively dispose (informally)

of any power of supervision over the entity from which it was the recipient of the entrustment or

order, because -as has been reiterated- it was not the holder of material competence

any on the aforementioned purposes or objectives of the treatment.

III.- The legal nature of IZENPE: its consequences in the present case.

IZENPE is a company that provides reliable identification services

electronically, in accordance with the provisions of Regulation (EU) 910/2014 (Regulation

eIDAS) and Law 59/2003, of December 19, on Electronic Signatures, and is considered

own medium personified, with instrumental character, indirect dependence and nature vicariate in relation to the entities or Public Administrations for which it acts. According to IZENPE's Statutes, the orders it receives from the contracting authorities of which it is own means will have an instrumental and non-contractual nature, will have an internal nature, dependent and subordinate; are articulated through mandatory execution orders, according to the instructions of the body that confers said order.

IV.- The nature of IZENPE as a provider of trust services, in the field of electronic transactions at a European or transnational level. according to the regulation eIDAS and its application to the present case. From what is established in this Regulation, IZENPE highlights the following:

a) These regulations must be applied in such a way as to comply with the principles relating to personal data protection. The aforementioned eIDAS Regulation and the RGPD are two sets related regulations, but which are not interchangeable, since both establish their respective singular assumptions of responsibility, confidentiality and mechanisms of security depending on the circle of attributions that are carried out in each case.

b) Thus, within the framework of the eIDAS Regulation, trust service providers must be liable for damages caused to any natural or legal person, and not only physical, as it happens in the scope of the RGPD.

c) The objective of the reiterated eIDAS Regulation is none other than "to provide a framework consistent with a view to guaranteeing a high level of security and legal certainty of trust services". And, for this purpose, the EU trust label is created and it is guaranteed

mutual recognition of electronic signatures. Likewise, certificates are regulated

qualified, the advanced electronic signature, the qualified and advanced electronic seal, etc.

d) Article 24 of the eIDAS Regulation expressly provides in section 2 that “The

Qualified providers that provide qualified trust services: (...) j) They will guarantee

lawful processing of personal data in accordance with Directive 95/46/EC”. Without

However, since the commercial company is a personified means of an entity that is

material owner of the competition and that defines the aims and objectives (why and for what) of the

data processing and its specific application (management and control of certain services

social), this referral to the data protection regulations must be applied to the delimitation

of the figures of person in charge and person in charge of the treatment, keys in the resolution of the

present case.

From the foregoing, IZENPE draws the following conclusions:

a) The eIDAS Regulation does not reflect, being previous, the differentiation of roles between responsible

and in charge of the treatment as has been subsequently specified by the RGPD, therefore

that the interpretation of its regulatory provisions must be appropriate to this new

reconfiguration of the role of both figures.

b) It is necessary to differentiate the responsibilities derived from a breach of the obligations

contained in the eIDAS Regulation, of those other responsibilities that occur

as a consequence of the processing of personal data, which will not be governed by

that set of regulations but by the RGPD.

c) Those cases in which the actions of the service provider entity must be differentiated.

trust services is of a general nature (issuance of identification systems that

are intended for services of a general nature or procedures before any entity or

public administration), of those other singular or specific actions that seek the

issuance of an identification system linked to the exercise of material competences

specific attributes attributed to a certain entity. In the first case, the provider of the

trust service will be considered responsible for the treatment; and not in the

second case, in which a control and management mechanism linked to the

competencies of the parent entity and not of the instrumental entity.

d) The 2014 Regulation is issued with a different European regulatory framework than the one

Data protection regulations currently govern: the RGPD. And, therefore, is the RGPD the

that defines the roles of data controller and data processor.

V.- On the other hand, it argues that, as a means of a Public Administration or

entity of Public Law, the sanctioning regime established for the

entity that formulates the order, that is, the one provided for in article 77 LOPDGDD. follow the

doctrine, supported by the Consultative Boards, according to which when an entity acts

mercantile as a personified means of a Public Administration, in practice it is

materially acting the Administration itself. And he adds that, if the non-imposition of

economic sanctions to a Public Administration is justified by the principle of Finance

Public, so that such sanctions do not revert to the public budget, the same argument

can be extracted when a commercial entity acts in the indicated context.

VI.- The effect on the principle of proportionality in data collection measures

biometrics in its fingerprint modality. The exceptional application of uptake.

Its purpose. The principle of proportionality in the strict sense. Application of the regulations of

1999 under the assumptions of the GDPR provisions.

The collection of biometric data can be lawful when there is consent of the interested party and

the judgment of proportionality is pertinent and not excessive.

From the point of view of the proportionality judgment, the biometric test was suitable, since served a legitimate purpose, and the information required in the RGPD was carried out (with interpretation difficulties due to its recent applicability); from the same point of view, understands completed the judgment of necessity, since the intervention measure is indispensable, not existing others with less interference that achieve the same result or end legitimate management simplification, fraud control and expense control; and as for the strict proportionality judgment, in which conflicting interests come into play, have been produced more benefits than burdens with the application of the treatment, both from the point of from a normative point of view (the advantages for the competent Administration and the users evident, in speeding up the procedure) and empirical, although the problem probably lies in the dimension of the sample carried out (collection of the fingerprints of the ten fingers of both hands), which must be assessed according to the empirical dimension of the problem exposed.

Also in this section, IZENPE reiterates that the processing of biometric data began with the regulatory framework prior to the RGPD, thus complying with the requirements established with the only doubt of the extent of the capture of the minutiae of the fingerprints on the fingers of both hands. Thus, it can arise if the treatment was pertinent and not excessive, but For this, it must be taken into account that it was done on a contingent basis and as a pilot test. This context limits or attenuates responsibility, since when the treatment began, it did not meant influencing sensitive data and, therefore, the disproportion of use did not have the consequences that derive from the application of the RGPD, also in what affects the principles of its article 5. Added to this are doubts about the scope of innumerable provisions of the new European regulatory framework, which are maintained in regard to the distribution of roles between controller and processor, especially in a case as the present in which different application circles of norms come into play in different material spheres and at different times.

It raises how a serious infringement can be attributed to a regulation that did not yet offer interpretive clarity, even more so in the absence of jurisprudence, and without considering that the entity acted with the legitimate expectation that its intervention was correct, in its condition of his own personified means that attended to the parcels and orders made. IZENPE cannot assume the condition of ultimate and exclusive responsibility for the design of the treatment, since it was not competent to exercise such functions nor did it have the powers to define the scope and goals of that treatment.

Likewise, it should be remembered that the identification system based on biometric factors in the LANBIDE's management scope only contemplated the pilot phase, whose objective was the evaluation and experimentation of the biometric technologies that were to form part of the final project, which has not yet been launched. Taking the minutiae of ten fingerprints had as objective the evaluation of the behavior of the system from the technological perspectives, user experience and from the field of data protection personal information. The aim was to adopt the optimal solution, reducing the error rate and the response time, associated with the minimization of biometric data collection. In this sense, the pilot project contemplated the identification based on the minutiae of a single fingerprint.

In any case, the project has been suspended since October 2019 pending the

approval of the corresponding law that legitimizes the implementation of the ID.

IZENPE provides a "Technical Report" regarding the information offered to interested parties,

in which it reproduces the text on the activation of the identification system included in the means of identification request forms, which requires the completion of the process by the user for its use, and stresses that these means involve the issuance of an electronic signature certificate in a secure centralized repository hosted on IZENPE.

EIGHTH: On 07/02/2020, a resolution proposal was formulated in the following sense:

1. That the Director of the Spanish Data Protection Agency sanction the IZENPE entity, for an infringement of articles 4.1 of the LOPD and 5 of the RGPD, typified in articles 44.3 c) of the LOPD and 83.5 a) of the RGPD, respectively, with a sanction of warning.

2. That the Director of the Spanish Data Protection Agency requires the entity IZENPE, so that in the term that is determined, it adapts to the protection regulations of personal data the treatment operations that it carries out, with the scope expressed in the Foundation of Law VIII. Specifically, it is proposed that IZENPE stop using illicit use of personal data related to the fingerprints of the interested parties, so you must keep the record of a single fingerprint, at your choice, and proceed to the elimination of the rest of the prints (those corresponding to nine fingers of the hands).

NINTH: The aforementioned resolution proposal was notified to the IZENPE entity, dated 07/16/2020, this Agency received a letter of allegations in which it reproduces, basically, its previous allegations, based on which it requests the filing of the performances:

I. After pointing out that the admission phase established in article 65.4 of the LOPDGDD was dispensable in this case, given that the claims were filed with the AVPD, which declared itself incompetent, refers IZENPE to the duration of the proceedings prior investigation, which article 67 of the LOPDGDD sets at twelve months. Understands IZENPE that it is necessary to differentiate between the formal and material dimensions of the case to conclude that,

Although this term was formally met, it can only be used when the

complexity of the investigation recommends extending it to its maximum limits, without

discretionary use can be made, as in this case, in which the opening of the

The procedure is substantially based on the actions carried out by the Agency

Basque, without the AEPD carrying out any material action of effective investigation,

having limited itself to requesting additional information or documentation. As a whole,

Considering all the indicated phases, the investigation actions reach almost twenty

months, and based on this concludes that the AEPD artificially dilated the period of

investigation, materially failing to comply with the maximum period established.

A case like this, in which two control authorities are involved, is not covered by the

cited article 67, but it is materially close to the relationship between the supervisory authority

of a Member State and the AEPD, when the latter receives a file admitted by

that. In this case, the twelve-month period should begin with the transfer of the

performances.

Regarding the consequences of this expiration, it cites the STS of May 13, 2019 (RC

2415/2016), which follows in the footsteps of another previous pronouncement (STS of May 6,

2015, RC 3438/2012), which includes a new doctrine by virtue of which the period

of previous actions must be projected on the effective performance of activities of

investigation without proceeding artificially to its prolongation, since this could imply incurring

in a fraud of law.

This temporary extension has harmed IZENPE, which has been accumulating the facts

proven subsequent data protection interventions and broadening the focus

quantity of possible infractions. In the draft resolution proposal itself, it is indicated

which are 3,624 records of forms prior to the date of entry into force (rectius,

of effectiveness or full applicability) of the RGPD, being as of 02/15/2019 10,738 users

the registration number.

II. The interest of the IZENPE entity in defining the position it adopts in the new

regulatory framework, as a commercial entity with the character of its own media personified by a

set of territorial public administrations and the instrumental entities that

depend on those, since data processing orders are constant, and

raises a number of preliminary questions:

a) Taking into account the different regulations that converge is important to define the

presumed responsibilities, especially considering the change brought about by the

RGPD in some aspects such as the position of the person in charge and in charge of the

treatment and the sanctioning regime applicable to public companies that have the condition

own media personified after the approval of Law 9/2017, of 8

November, of Public Sector Contracts (LCSP), which accentuates the position of dependency

functional of these means, so that they cannot be attributed a more

burdensome in terms of personal data protection than the parent company, which is the one that

it has the material competence and the one that defines the ends.

It is not enough for this, as the AVPD did and then ratifies the AEPD, with the mere formal transfer

of collaboration agreements that were signed in 2017 and were extended

subsequently, since these agreements were drafted in accordance with the LOPD and the

regulatory regulations that developed it (when speaking of responsible for files). One time

entry into force of the LCSP the only way to formalize these relations between LANBIDE and

IZENPE were the personified half-own commissions, something that -due to unrelated circumstances

to this company - was not formalized until November 30, 2018 and, in addition, maintaining,

also erroneously, the roles of data controller and data processor

cross-processing (that is, assigning the role of data controller to

who should be in charge and vice versa, as a consequence of the automatic transfer of the

figure of the person in charge of the file to that of the person in charge of treatment, who are not at all

coincident nor do they have to have that correspondence).

b) According to article 2 of Law 2/2004, on personal data files of

public ownership and creation of the Basque Data Protection Agency, this data protection authority

control has no competence to purge the responsibilities that derive from a

treatment carried out by a public commercial company, although the

shares or participations correspond entirely to Basque public authorities, therefore

that would be subject to the control and supervision of the AEPD.

This situation changes with the LOPDGDD, whose article 57 establishes that the authorities

regional authorities for data protection may exercise the powers established in the

articles 57 and 58 of the RGPD when, in accordance with regional regulations, they refer to

“treatments for which the entities that are part of the public sector of the

corresponding Autonomous Community (...) included in its territorial scope (...)”. In these

moments since Law 2/2004 had not been modified, the competition would continue to be

temporarily from the AEPD, but the fundamental purpose of this generic attribution is not

may be other than broadening the focus of supervision, as is the case, to all those

public companies that are dependent, linked or affiliated (for control purposes)

economic-financial) to a parent Administration and that act as their own means

personified of this or of the Administrations that make up the shareholders and the Board
Administration of such businesses. The link of dependency narrows and attracts to itself
the competence of the regional control authority to an institutional sphere that until
now he did not compete.

This also has close connections with the scope of the exceptional regime in matters of
of sanctions to public administrations and dependent entities that is foreseen in the
article 77 LOPDGDD, whose institutional logic is without foundation unless it is
justify that the medium itself personified as long as it acts in accordance with the order
received cannot be sanctioned autonomously and must be sanctioned by the parent Administration.

III. Considers it necessary to define conceptually and normatively some arguments and
expressions included in the motion for a resolution:

a) The statement is not true: “IZENPE has stated that it was decided to implement the system in
LANBIDE on an experimental basis for all workers and users of the service (collective
close to 300,000 people), in order to improve, simplify and make more efficient the management
administration, thus responding to the needs of society”.

The impersonal expression “it was decided” cannot be used, since the holder of the
material competition was and is LANBIDE, then IZENPE acting as its own medium and
technical service and, from the entry into force of the LCSP 9/2017, as its own means
personified. LANBIDE is the interested party for the purposes indicated above.

b) On the proven facts concluded from the formalized documents, according to the
which “IZENPE declares itself responsible for the treatment (also of the file) and LANBIDE
intervenes as the person in charge for the mere collection and validation of the data and its subsequent
shipment to IZENPE”, indicates this entity that the Agency has not made any effort
interpretation to warn (“a kind of lifting of the veil”, says IZENPE) that this
company could not be responsible for the treatment in accordance with the RGPD. Also,
considering it as in charge of the treatment does not affect or modify a posteriori the rights

of the interested parties, as the motion for a resolution points out, who are in no way affected

for the change of roles.

c) Considers the interpretation of the figure of the person responsible for the treatment contained

in the RGPD the statement made in the proposal that reads as follows: “It is also convenient to have

present the definition of data controller expressed in article 4 of the RGPD,

that considers as such not only the one who defines the ends, but also the one who enables the means

for the treatment, as IZENPE does in this case”. This article requires that the responsible

“determine the purposes and means of the treatment”, not only the means, or there would be a risk of

dilute the differentiating profiles of responsible and in charge. That reading would be

particularly serious in relation to the personified means themselves.

It cites Recital 74 of the RGPD and adds that it cannot be responsible for the treatment

who in no case defines the ends, even if he puts means for those ends to be fulfilled,

because in that case it would be responsible for measures that are beyond its scope of action

material, apart from the fact that he responds as the person in charge of the assigned functions.

In no case can IZENPE be considered responsible for the treatment, no matter how

that such condition was mistakenly included in the documents that were provided by the

AVPD to the sanctioning file. From the full applicability of the RGPD, IZENPE will not

could have such a condition because it is materially impossible for the company to define the purposes of the

treatment when it is not the holder of the substantive competence that such treatment serves:

“improve, simplify and make more efficient the administrative management” of a material scope

such as active employment policies and income guarantee income in which there is no

has, not even remotely, any possibility of intervening, since it is not within its corporate purpose

nor is it proper to its nature as a personified proper medium.

d) The above approach was not taken into account by the AVPD when it decided to reject the

claims.

Derived from a formal document that LANBIDE, an entity that set the goals and benefited

of the results of the treatment, it is only a registration entity is a conclusion

rushed, since the personal data protection regulations cannot be interpreted

exclusively from the material regulation in that area, but through the whole of the

current legal system, so it must be specified, on the one hand, the jurisdiction

material of the entity that defines the purposes and means of the treatment, which is LANBIDE; and by

another, that IZENPE is considered to be the personified medium of the

Public Administrations or dependent entities that carry out "commissions" and is, by

consequently, subject to a "control analogous" to that which the parent entity (LANBIDE) exercises over

its own administrative services, so it lacks absolute and total autonomy

(also of competence) to define the purposes of the treatment and the means that it puts into

action are always in the service of such ends.

e) Regarding the reformulation of the roles already announced, IZENPE clarifies that its purpose is to leave

proof of the following:

. That until May 25, 2018, he recognized in the Collaboration Agreement that he had the

condition of file manager, although even then it was its own medium and technical service

or LANBIDE's own personified medium in this case. The responsibilities that

could

derive from the actions carried out in such period were in the condition of such, but never of

responsible for the treatment.

. That as of May 25, 2018, IZENPE could not be considered a

responsible for the treatment, in accordance with the foregoing (it does not have the competence

material that determines the ends and acts in its capacity as its own personified means of

the entity that owns the competition).

. That such "reformulation" of roles does not affect the rights of the claimants who formulated

timely claim, as either LANBIDE or IZENPE, in their roles

formal or material (whether in charge or responsible and vice versa), they would respond to the

hypothetical irregularities of the treatment carried out.

. It is necessary to define the figures of responsible and in charge of the treatment in the

resolution of this procedure, which will have important general repercussions and will set

doctrine in this regard, making it clear that the definition of the ends are necessarily linked

with the material skills that an entity develops and not only with the means that

facilitates to start or apply a certain treatment; and without forgetting that IZENPE

is a personified own medium controlled by a parent entity in a manner analogous to control

that it exercises over the entities that depend on it (improper hierarchy).

. That the control authorities exercise differentiated spheres of competence based on

administrations and entities of the public sector in question, although this situation

may be altered in the future by the provisions of article 57.1 LOPDGDD.

. IZENPE has the nature of its own personified medium and its financial resources depend

exclusively from the Public Treasury of the different entities to which they lend these

mediated services, so it makes no sense to impose administrative fines

(it is a public company of an instrumental nature, subject to “analogous control” to that existing at

another administrative service and financed exclusively by “orders” that determine what

should be done, how and for what purpose).

Based on the foregoing, you request:

a) to proceed, for formal reasons, to file the proceedings, having to estimate the

expiration of the procedure, which does not prevent, in principle, that the AEPD can reactivate it

in the terms established in the LPACAP; in particular the artificial extension of the

previous investigative actions, which have lasted beyond the necessary period.

b) Subsidiarily, proceed, for material reasons, to archive the actions in the

terms set forth in their pleadings.

In the event that neither of the two previous requests are accepted, the following is requested:

a) That the resolution accepts exclusively the responsibilities of IZENPE as

responsible for the treatment file until May 25, 2018, recognizing

also that, during that period, it had the status of its own means and technical service or,

in his case, LANBIDE's own personified medium, and that his performance was instrumental and

non-material, lacking the substantive competencies whose efficiency was intended to be improved.

b) That, as of May 25, 2018, IZENPE could not materially have the condition

responsible for data processing, considering that it did not define the purposes of the

treatment.

c) That, the sanctions that, in his case, can be applied to him should be as a manager

of the treatment and never as the person in charge of the treatment, since this consideration was

mistakenly attributed by a mechanical translation of the figure responsible for

file to that of data controller, when the latter has been redefined

completely after the full applicability of the GDPR. Such a consideration is also very

important for the company given its condition as its own media personified by different

Public Administrations and entities at their service.

d) That all of the above would not affect the rights of the claimants in any case. Without

despite the fact that the initial claim of such claimants was filed with LANBIDE, which

exercised effective competition and carried out the entrustment (formulated as "agreement of collaboration"), in accordance with the TRLCSP of 2011, or the "assignment", in accordance with the LCSP of 2017.

In view of everything that has been done, by the Spanish Data Protection Agency

In this proceeding, the following are considered proven facts:

PROVEN FACTS

1.- In 2002, the General Administration of the Autonomous Community of Euskadi and the Provincial Councils, through their respective public limited companies information technology, formed the company Ziurtapen eta Zerbitzu Enpresa-Empresa de Certification and Services, Izenpe, S.A. (IZENPE) for the development of identification electronically, as its own system of identification and electronic signature.

As stated in its Articles of Association, which are declared reproduced for evidentiary purposes, IZENPE's corporate purpose is the issuance and management of media and communication systems electronic identification for electronic identification, authentication, signing and/or sealing, to public or private persons or entities.

It is considered a trusted service provider (electronic identification, signature electronics, etc.) according to Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014 regarding electronic identification and identification services trust for electronic transactions in the internal market and repealing the Directive 1999/93/EC; and it also has the condition of a personified medium of the entities that participate in its capital, as determined in Law 9/2017, of 8

November, of Public Sector Contracts, by which they are transposed into the legal system

Spanish the Directives of the European Parliament and of the Council 2014/23/UE and 2014/24/UE, of

February 26, 2014.

2. IZENPE has stated that, since 2016, in its capacity as media outlet for the

Administrations that participate in its capital, by order of the same, and in the field of

eIDAS Regulation, has been developing the project for the issuance of means of identification

with a centralized certificate (in the cloud) for individuals, with which it is intended to provide

citizenship of a means of identification, always voluntary, easy to use in relationships

telematics with the Basque Administrations according to the requirements of each procedure and/or

service.

It has developed two systems (B&K and B&K Q) that allow the identification and signature

electronic, consisting of a reference number, password, set of coordinates and

electronic signature certificate.

. B@K is defined as a means of low-level electronic identification, made up of

a reference number matching the DNI/NIE/Passport of the user and a

password; and an unqualified certificate issued in a centralized repository that

It will be used for signing acts.

. B@K Q is defined as a mid-level electronic identification medium, consisting of

by a reference number that matches the DNI/NIE/Passport of the user and a

password; a set of coordinates with 16 positions; and a qualified certificate of

electronic signature issued in a centralized repository of IZENPE that will serve for

signing acts.

IZENPE has stated before this Agency that the commission for the provision of various services related to the identification and electronic signature was carried out by Resolution of 11/14/2017 (declared reproduced for evidentiary purposes), of the Director of Services of the Department of Public Governance and Self-Government, in whose structure is integrated the Department of Attention to Citizenship and Innovation and Improvement of the Administration, which has attributed "the effective implementation in the public administrations of the Administration electronically in administrative procedures and in the management of public affairs", as well as such as, "the declaration and management of the common services of electronic processing of the Public Administration of the Autonomous Community of Euskadi".

The electronic services to be provided by IZENPE will allow the General Administration of the Autonomous Community of Euskadi to interact with citizens, companies private and with the rest of Public Administrations. Among other electronic services, the The purpose of this assignment is the integrated system of eIDAS keys and includes the creation, verification and validation of identification keys and their preservation.

3. Lanbide-Basque Employment Service, an autonomous administrative body attached to the Department of Employment and Social Policies, and the entity IZENPE signed a collaboration agreement, of 10/26/2017 (published on 03/26/2018), which is declared reproduced for evidentiary purposes, for the implementation of means of identification emails of natural persons (workers and users of Lanbide - claimants of employment in general, participants in training activities and guidance services, as well as applicants for social benefits of the Income Guarantee Income and the Complementary Housing Benefit; It is a group close to 300,000 people) based on the collection of biometric data. It is intended to include elements more secure identification methods, such as biometric factors, including facial features and fingerprints. According to its descriptive part, the agreement is framed in Law 39/2015, to

deepen the implementation of electronic administration, and the Regulation (EU)

910/2014.

Through Resolution 156/2018, of November 26, of the Director of the Secretariat of the

Government and Relations with Parliament, the publication of said agreement of

collaboration under the title "Collaboration agreement for the deployment of the pilot project of

electronic means of identification based on the collection of biometric data".

The agreement states that LANBIDE has established the operating key as a means to

prove identity and intends to facilitate an interoperable system that allows

users of its services interact with any administration with which

legal and security guarantees; and that it is intended to incorporate new factors of

identification to the two systems developed by IZENPE (B&K and B&K Q), such as those

biometric factors, among which he cites facial features and fingerprints.

The following is stated in its clause:

. Izenpe is a trusted service provider. Under this agreement, Lanbide

acquires the status of Izenpe registration entity for the issuance of means of

digital identification and electronic signature B&K and B&K Q. in relation to natural persons

users who request means of identification issued by IZENPE.

LANBIDE will carry out the following actions: verify identity; capture the footprints

digital; face photography; signature of the application for issuance of B&K and B&K Q; record the

biometric data obtained (fingerprints and photo) in the identity management system

Izenpe (identity file) IZENPE identity file; send to Izenpe the

request for the issuance of B@k and B@k Q signed by both the applicant and the operator of

Lanbid.

. Valid one year.

. IZENPE provides the training and provides the software.

. Data protection: IZENPE is responsible for the files declared before the AEPD,

that treat the data of the different agreed services and Lanbide intervenes as manager

of the treatment, in accordance with article 12 LOPD.

On 10/15/2018, the entities IZENPE and LANBIDE signed an Addendum to the

Collaboration agreement of 10/26/2017, which is declared reproduced for evidentiary purposes,

for the extension of the same for one year from 10/26/2018 and to adapt to the RGPD

the wording of the seventh clause, relating to data protection, which is as follows:

“1.- Izenpe regarding the data provided by the applicant of the media

identification, has the status of Data Controller and identifies this service in

the scope of the following treatment:

Treatment: Management of means of identification based on biometric factors.

Data subject to treatment: Identification. Special categories of data: biometric data.

Storage period: 7/15 years, depending on the non-qualified/qualified means of identification,

from the formalization of the request.

2.- When Lanbide acts as a Registration Entity, it will acquire the status of Responsible for

Treatment of the personal data that the applicant provides.

This treatment will consist of the collection and validation of the data and its subsequent sending to

Izenpe. For the execution of this benefit, Izenpe will provide Lanbide with access to the

necessary applications.

3.- Lanbide, as well as its staff, acquires the following obligations:

a) Use the personal data subject to treatment, or those collected for inclusion, only

for the purpose of this agreement.

In no case may you use the data for your own purposes.

b) Treat the data in accordance with what is determined by Izenpe.

(…)".

4.- Due to the claims that have given rise to these actions, which

were initially presented to the Basque Data Protection Agency, the services

of the same inspection carried out an inspection in one of the offices of LANBIDE. In

the Inspection Act prepared, dated 07/06/2018, which is hereby reproduced for purposes

evidence includes the following:

<<... information is requested on the process of collecting fingerprints, offering the staff

of Lanbide to carry out a simulation of the complete process, which entails the treatment of the

DNI/NIE/Passport, the collection of the fingerprint of the ten fingers of the hands and the image

facial…

Upon questioning from the acting inspectors, it is reported that there are currently 43 offices of

Lanbide, with 600 posts and ten operational posts for the pilot experience of collecting

fingerprints, having collected to date around 5,900 biometric data.

People who come to the office are seeking employment and guarantee income

of income and the collection of your biometric data is voluntary. When the

person goes to the office to carry out some paperwork, once it has finished, they are

informs of the future need for digital identification of users, after which, it is sent to the

pick up point…

Lanbide personnel inform the inspectors that the fingerprint and facial data of the

users are collected by Lanbide on behalf of the certification and services company

Izenpe, S.A., which is the one who stores the data. The forecast is to expand the collection through

fingerprint readers in all 43 Lanbide offices by the end of 2018. Currently,

Lanbide does not use biometric data for identification purposes of the users of its

services as the system is not yet operational.

Lanbide staff, at the request of the inspectors, gives them the informative brochure

on the collection of biometric data, the informative clause that is delivered in the offices

and the model for exercising the right of cancellation>>.

(Subsequently, in its response to the AEPD on 12/05/2018, IZENPE stated that, until

November 2018, approximately 9,000 people requested this means of identification

with biometric factors. And in his letter of 02/18/2019, he declared that until 02/15/2019 the

number of users from whom biometric data had been taken amounted to 10,738

users, of which 3,624 are prior to the date of entry into force of the RGPD).

5. During the inspection carried out by the Basque Data Protection Agency on the date

07/06/2018, it was found that the notice boards of the Lanbide office contained

exposed informative posters with the following text:

“Soon it will be necessary to digitally identify Lanbide users.

For this reason, we invite you to stop by the collection post once your attention is over.

biometric data…”.

(IZENPE has declared before this Agency that the text of the informative poster was replaced in

July 2018 by the following: "In this office a data collection station has been installed

biometrics for the digital identification of LANBIDE users.

If you are interested, we invite you to go through booth nº… to obtain the information

that you need and, where appropriate, carry out the necessary procedures”).

. Likewise, during said inspection, the document used to provide the

interested parties information on the protection of personal data and collect their

consent to the collection of your data. The content of this document is

Next:

“Izenpe informs you that through the biometric data (fingerprints and photograph) that

are going to register, you will be able to have a means of electronic identification that will allow you to

interact with the Basque administrations.

In addition, and depending on the level of security required by virtue of the administrative procedure, said

biometric data will be able to complete the use of B@K electronic identification means

and/or B@K Q.

This means of identification consists of fingerprints, a facial photograph of the

applicant and the following personal data:

The applicant must fill in the following data_all the data are from

mandatory completion_.

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

Surnames

Name

ID/Passport number

Date of Birth

Email

contact mobile phone

Informative clause (Basic information on data protection)

Responsible: Ziurtapen eta Zerbitzu Enpresa-Certification and Services Company, Izenpe,

S.A.

Purpose: Provision and management of services associated with means of identification

electronics

Rights: access, rectification and cancellation through c/… or info@izenpe.com.

Additional Information

Http://www.izenpe.eus/contenidos/informacion/doc_comun/es_def/adjuntos/DOC_P_PDS_v1.

0.pdf

Date and signature of the applicant.

(In the copy of this initial form provided by IZENPE with its letter of 02/18/2019

it is reported that the electronic identification, B@k is formed by a reference number

matching the DNI/NIE of the user and a password assigned by IIZENPE; a

non-qualified certificate issued in a centralized repository that will serve for the acts of

signature; and biometric data (fingerprint and photograph). The medium B@kQ is formed,

in addition, by a set of coordinates with 16 positions and a qualified signature certificate

issued in a secure centralized repository of IZENPE, the "cloud", which will serve

for signing acts).

. Earlier means of identification request forms were later

modified. The new versions contain the basic information and a link to the web for

the additional information. The first section of this application explains that the means of

identification consists of a reference number or non-qualified certificate or a set

of coordinates (according to the type of medium) and it is added that “in addition, it can be complemented

by other biometric authentication factors such as fingerprint and/or photograph” (only

reference to the biometric data that appears in these application documents).

In these new B&K and B&K Q application forms, interested parties are informed that

These are means of electronic identification that will allow you to interact with the

Basque administrations and it is detailed that these means of identification are made up of

a reference number (coinciding with the DNI/NIE/passport of the user and a

password), an unqualified certificate issued in a centralized repository that will serve

for signature acts (B@K) or a set of coordinates with 16 positions and a certificate

certificate of electronic signature issued in a centralized repository of IZENPE that will serve

for signature uses (B@K Q). In both cases, moreover, the means of identification may

be supplemented by other biometric authentication factors such as fingerprint and/or

photograph (only reference to the biometric data that appears in these identity documents)

request).

It is added that when the holder of B@k or B@K Q uses the medium in question for his

identification before an electronic service, Izenpe, in the event that the authentication is

correct, will offer the body responsible for the service the result of it.

By signing the corresponding applications, the undersigned declares that he has read and accepts the

Terms and Conditions of use of this means of identification published in

www.izenpe.eus/condicionesuso.

In the aforementioned forms, personal data related to name, surnames, DNI or

passport, date of birth, email and contact mobile phone.

On the back of these applications, "Basic information on data protection" is offered, with

the following content:

“Responsible: IZENPE

Purpose: Issuance and management of the life cycle of the requested means of identification.

Legitimation: consent of the interested party

Recipients: it is not expected to transfer or communicate data to third parties, except legal provision, nor

make international transfers.

Rights: Right to obtain confirmation about the processing of your data that is

carried out by Izenpe.

You can exercise your rights of access, rectification, deletion and portability of your data,

of limitation and opposition to their treatment, not to be the subject of decisions based solely on

in the automated processing of your data, as well as to withdraw your consent in

any time and to file a claim with the Spanish Agency for the Protection of

Data.

You can exercise these rights by request to the postal address C/ Beato Tomás de

Zumarraga no. 71, 1st floor. 01008 Vitoria-Gasteiz or electronically

datos@izenpe.eus as indicated in the additional information.

Additional information: available at www.izenpe.eus/datos".

By signing the application (includes a space for signature), as indicated on the application, the

interested party consents to IZENPE the treatment of personal data referring to the

means of identification requested.

. In its letter of 02/18/2019, IZENPE has stated the following:

The number of users from whom biometric data was taken before the modification

of the application forms is 10,378 records, and 320 more records after their modification.

IZENPE warns that the initial forms were used from 10/26/2017 and that these

were modified on 12/04/2018, although, due to a technical incident, the

new models have not been used until February 5, 2019.

FOUNDATIONS OF LAW

Yo

By virtue of the powers that article 58.2 of the RGPD recognizes to each Authority of

Control, and according to what is established in articles 47, 48, 64.2 and 68.1 of the LOPDGDD, the

Director of the Spanish Agency for Data Protection is competent to initiate and

resolve this procedure.

Article 63.2 of the LOPDGDD determines that: "The procedures processed by the

Spanish Agency for Data Protection will be governed by the provisions of the Regulation (EU)

2016/679, in this organic law, by the regulatory provisions issued in its

development and, in so far as they are not contradicted, on a subsidiary basis, by the general rules

about administrative procedures.

II

Beforehand, it is appropriate to analyze the exception raised by IZENPE in its

brief of allegations at the opening of the procedure, regarding the possible expiration of the

preliminary investigative actions. This entity stated that there is no evidence

action of specific investigation, apart from the transfer of claims, so

that it is not possible to determine compliance with the twelve-month requirements established

in article 67.2 of the LOPDGDD. He adds that he was also unaware of the admission to

claims processing.

The procedures carried out by this Agency to which IZENPE refers in its allegation

above have to do with the process of admission to processing of the claims received,

which included for four of the five claims received their transfer to the person in charge,

prior to the agreement to admit the claim.

In accordance with the provisions of article 55 of the RGPD, the Spanish Agency for

Data Protection is competent to perform the functions assigned to it in its

Article 57, among them, that of enforcing the Regulation and promoting the awareness of the

responsible and those in charge of the treatment about the obligations that incumbent on them,
as well as dealing with the claims presented by an interested party and investigating the reason for the
themselves.

Correlatively, article 31 of the RGPD establishes the obligation of those responsible
and those in charge of the treatment to cooperate with the control authority that requests it in the
performance of their duties. In the event that they have appointed a delegate of
data protection, article 39 of the RGPD attributes to it the function of cooperating with said
authority.

Similarly, the domestic legal system, in article 65.4 of the LOPDGDD, has
foreseen a mechanism prior to the admission for processing of the claims that are formulated
before the Spanish Agency for Data Protection, which consists of transferring the same
to the data protection delegates designated by those responsible or in charge of the
treatment, for the purposes provided for in article 37 of the aforementioned rule, or to these when not
they have been designated, so that they proceed to the analysis of said claims and to give them
response within one month. It is an optional procedure, so that this
transfer is carried out if the Agency deems it so, as decided in this case.

Thus, in accordance with this regulation, prior to admission for processing of
the claims that have given rise to this procedure, the transfer of the
same to IZENPE so that it could proceed with its analysis, respond to this Agency and
inform the claimants of the decision adopted in this regard.

The result of said transfer did not make it possible to understand that the claims of the
claimants. Consequently, for the purposes provided in article 64.2 of the LOPDGDD,

Through two separate agreements dated 01/09/2019, the Director of the Spanish Agency for Data Protection agreed to admit the claims submitted for processing.

On this issue, IZENPE has stated in its allegations to the proposal of resolution that the transfer process was dispensable in this case, given that the Complaints were filed with the AVPD, which declared itself incompetent. Nevertheless, There is no legal consequence of this fact or the actions carried out by the AVPD prior to the referral of the claims to the AEPD, regarding the formalization or not of the aforementioned procedure, or the opportunity it represents for the person responsible for responding to the claims and the possibility that this entails to prevent them from taking the course provided for in Title VIII of the LOPDGDD.

This admission for processing was agreed upon, which was notified to the claimants, and not to IZENPE, in accordance with the provisions of article 65.5 of the LOPDGDD, began previous investigation actions indicated with the number E/00995/2019. Within these actions, dated 02/04/2019, the inspection services of this Agency sent IZENPE a request for information, in which said reference number appears and it is expressly indicated that said request is made "Within the framework of the actions practiced by the Subdirectorate General for Data Inspection in order to clarify the terms of some facts susceptible of possible infraction to the current regulations of Data Protection and of which this Spanish Agency of Data Protection" and in use of the powers conferred by article 58.1 of the RGPD and the Article 67 "Preliminary investigation actions" of the LOPDGDD.

This being the case, it turns out that the previous research actions carried out were known by IZENPE.

On the other hand, it should be noted that at the time the notification of the opening of this procedure, on 12/19/2019, the term of

duration provided for in article 67.2 of the LOPDGDD, counted from the date of the agreement of admission to process.

IZENPE does not share the above conclusion. In his arguments to the proposal of resolution states that the twelve-month period can only be used when the complexity of the investigation recommends extending it to its maximum limits; and adds that the opening agreement is based on the actions carried out by the AVPD, without the AEPD carried out any material action of effective investigation, having been limited to requesting additional information or documentation (cites the STS of 05/13/2019 -RC 2415/2016-, which follows another previous pronouncement -STS of 05/06/2015, RC 3438/2012-, noting that it includes a new doctrine by virtue of which the period of proceedings must be projected on the effective performance of research activities without proceed artificially to its prolongation.

Understands that the referral of claims to the AEPD by another control authority assumes that the calculation of the twelve-month period begins with the transfer of the proceedings and concludes that the AEPD artificially dilated the investigation period to almost twenty months, harming IZENPE, which has been accumulating the proven facts subsequent interventions on data protection and broadening the quantitative focus of possible infringements (for example, in number of registered users).

However, the rule clearly establishes the different actions that can

be followed once a claim is received and the procedures to which it may give rise, positively establishing the period of duration and the computation of that period for each

performance. In what is of interest now, the decision on admission or non-admission for processing must be notified to the claimant within three months from when the claim was received in the agency; Once the claim has been admitted for processing, actions may be taken preliminary investigations, with a duration not exceeding twelve months, counted from the date of the admission agreement. The computation of the time used to evaluate the admissibility of the claim is excluded from the calculation of the period available for the development of research actions.

The norm does not distinguish any special rule for claims presented before the regional data protection authorities that are finally sent to this Agency for examination; nor is the duration of the preliminary actions subject to any condition regarding its development, whether formal or material.

On the other hand, it is necessary to specify that the Judgments of the Supreme Court cited by IZENPE are not refer specifically to this last issue, nor does it conclude what IZENPE said about the requirement to link the period of preliminary investigation actions to the completion effectiveness of research activities. This Judgment analyzes a possible infringement of the Articles 20.6 of Royal Decree 1398/93, of August 4, approving the Regulation of the Procedure for the Exercise of the Sanctioning Power and 42.3.a of Law 30/1992, regarding the computation of the term to assess the expiration of the sanctioning file. The appellant argued that the computation of that period should start on the date of formulation of the prior complaint and the Court declared that the term available to the Administration to resolve begins with the agreement to initiate the file, being therefore excluded from said computation the period of time elapsed from the date of the news of the event offender and, where appropriate, the employee in the previous actions. Add the judgment cited Next:

“The appellant maintains that with this interpretation the Administration is being granted a unlimited term to initiate the procedure. However, this Chamber has declared that this

period prior to the initiation agreement <<... must necessarily be brief and not cover up a

artificial way of carrying out acts of instruction and masking and reducing the duration of the

subsequent file >> (judgment of May 6, 2015, appeal 3438/2012,

FJ 2nd, which cites, in turn, a previous pronouncement on the same line of

reasoning)".

Therefore, the cover-up of investigative acts prior to the

beginning of the procedure in order to subtract them from the computation of the expiration period, but

this Judgment does not contain any pronouncement on what is alleged by IZENPE in relation to

with previous investigation actions.

No prejudice is translated for IZENPE from the follow-up of the procedures foreseen in

the regulations outlined.

III

The LPACAP dedicates Chapter II of Title I to the “Identification and signature of the

interested in the administrative procedure”, articles 9 to 12.

Article 9 of the aforementioned Law establishes that "Public Administrations are

obliged to verify the identity of the interested parties in the administrative procedure,

by checking your name and surnames or denomination or company name, according to

corresponding, that appear in the National Identity Document or identification document

equivalent". This precept, in section 2, refers to the systems that may be used by

interested to identify themselves before the Public Administrations:

"two. Those interested may identify themselves electronically before the Public Administrations

through the following systems:

a) Systems based on qualified electronic signature certificates issued

by providers included in the ‘‘Trusted list of service providers of

certification".

b) Systems based on qualified electronic seal certificates issued

by providers included in the ‘‘Trusted list of service providers of

certification".

c) Concerted key systems and any other system that the Administrations

considered valid in the terms and conditions established, provided that they have

a prior registration as a user that allows guaranteeing your identity, prior authorization by

part of the General Secretariat of Digital Administration of the Ministry of Territorial Policy and

Public Function, which may only be denied for reasons of public security, prior

binding report from the Secretary of State for Security of the Ministry of the Interior. The

Authorization must be issued within a maximum period of three months. Without prejudice to the

obligation of the General Administration of the State to resolve in term, the lack of resolution

of the authorization request will be understood to have dismissal effects.

The Public Administrations must guarantee that the use of one of the systems

provided for in letters a) and b) is possible for any procedure, even when it is admitted

for that same procedure any of those provided for in letter c).

On the other hand, 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 internal market and repealing the Directive

1999/93/CE, in its Chapter I, dedicated to the "General Provisions", establishes the

Next:

“Article 2. Scope of application

1. This Regulation applies to notified electronic identification schemes

by the Member States and trust service providers established in the

Union.

2. This Regulation does not apply to the provision of trust services used

exclusively within closed systems resulting from national law or agreements

among a defined set of participants.

3. This Regulation does not affect national or Union law relating to the

conclusion and validity of contracts or other legal or procedural obligations

relating to form".

"Article 5. Treatment and protection of data

1. The processing of personal data will be in accordance with the provisions of the Directive

95/46/EC".

In this regard, Recital 11 of the aforementioned Regulation states the following:

"This Regulation must be applied in such a way as to fully comply with the principles

regarding the protection of personal data established in Directive 95/46/CE of the

European Parliament and of the Council. To this end, given the principle of mutual recognition

established by this Regulation, authentication for the purposes of an online service must

involve exclusively the processing of identification data that are appropriate,

relevant and not excessive for granting access to the online service in question.

On the other hand, trust service providers and the supervisory body must

also respect the requirements of confidentiality and security of the treatment provided for in

Directive 95/46/EC".

And article 24 of this Regulation, included in Chapter III, referring to the Services

of Trust, establishes the following:

“Article 24 Requirements for qualified trust service providers

1. When issuing a qualified certificate for a trust service, a qualified provider

of trust services will verify, by the appropriate means and in accordance with the Law

identity, and, if applicable, any specific attributes of the natural or legal person

to which a qualified certificate is issued.

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

either directly or through a third party in accordance with the

National law:

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

either

b) remotely, using means of electronic identification, for which the

guaranteed the presence of the natural person or of an authorized representative of the person

prior to the issuance of the qualified certificate, and that meet the requirements

set out with Article 8 with respect to "substantial" or "high" safety levels, or

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

certificate issued in accordance with letter a) or b), or

d) using other nationally recognized methods of identification that provide a

security equivalent in terms of reliability to physical presence. The equivalent security

will be confirmed by a conformity assessment body.

2. Qualified trust service providers who provide trust services

qualified:

(…)

f) use reliable systems to store the data provided to them in a verifiable manner,

so that:

i) are available to the public for retrieval only when the

consent of the person to whom the data corresponds,

ii) only authorized persons can make annotations and modifications in the data

stored,

iii) the authenticity of the data can be verified;

g) take appropriate measures against falsification and theft of data;

h) record and keep accessible for an appropriate period of time, including

When the activities of the qualified provider of trust services have ceased, all

the relevant information regarding the data issued and received by the provider

qualified trust services, in particular for the purpose of serving as evidence in

legal proceedings and to ensure continuity of service. This log activity

it may be done by electronic means;

(…)

j) will guarantee lawful processing of personal data in accordance with Directive

95/46/CE;

k) in the case of qualified trust service providers that issue certificates

qualified, will establish and keep up to date a database of certificates".

In accordance with the aforementioned Regulation (EU) 910/2014, service providers of

confidence are subject to the supervision of a body designated by the Member State, and

This supervisory body is obliged to "cooperate with the protection authorities

of data, for example by informing them of the results of audits of providers

qualified trust services, in the event that the rules on

Personal data protection. The provision of information must include, in

particular, security incidents and data breaches

staff".

It corresponds to the providers of trusted services the rendering of accounts in

in relation to its operations and services.

It also establishes the mutual recognition of means of identification

between Member States for the purposes of cross-border authentication. In this

sense, the systems notified to the Commission shall be interoperable.

In accordance with the foregoing, the trust service provider is obliged to

record and store the data, as well as the maintenance of the database,

It is up to you to guarantee the lawful processing of personal data.

IV

In the present case, IZENPE carries out processing of identifying personal data and

of contacts of users of the Basque service LANBIDE, to which it adds the taking of a

photograph, which is also considered personal data, as well as fingerprints

fingerprints that are incorporated as an identification factor.

The collection of this data is carried out in order to establish a system

of electronic means of identification within the framework of the standards outlined in the

foundation of previous, and takes place in a period before and after 05/25/2018, date to

from which the RGPD is applicable.

Data processing prior to that date is subject to the

principles and rules established in Organic Law 15/1999, of December 13, of

Protection of Personal Data (hereinafter LOPD), and among them, the principles

of relevance and proportionality, established in article 4.1 of said Organic Law.

“Article 4. Data quality

1. Personal data may only be collected for processing, as well as

submit them to said treatment, when they are adequate, pertinent and not excessive in

relation to the scope and the specific, explicit and legitimate purposes for which it is

have obtained”.

This article 4 of the LOPD, with the name "Data Quality", is the first

precept of title II dedicated to the "Principles of data quality", which derive from the right

essential to data protection. Section 1 of article 4 of the LOPD begins

establishing that personal data may only be collected for processing,

as well as subjecting them to said treatment, in accordance with a series of criteria, which are

summarized in the principle of proportionality, compliance with which is required of the person responsible for

treatment.

This article relates the principle of proportionality in data processing

of a personal nature and the limitation of purposes, which prevents the treatment of those that are not

are necessary or proportional to the purpose that justifies the treatment, resulting

contrary to the LOPD the treatment of excessive data. Consequently, the treatment of

data must be relevant and not excessive in relation to the purpose pursued. they can only

be subjected to treatment those data that are strictly necessary for the

purpose pursued. On the other hand, compliance with the principle of proportionality not only

must occur in the field of data collection, but must be respected,

likewise, in the subsequent treatment that is carried out on them.

This criterion is also included in article 6 of Directive 95/46/CE and

is reflected in Convention 108, of the Council of Europe, of January 28, 1981, for

the protection of individuals with respect to the automated processing of personal data

personal, whose article 5.c) indicates that "the personal data that are the subject of a

automated processing... will be adequate, relevant and not excessive in relation to the

purposes for which they have been registered.

They are the same principles included in Recital 28 of the aforementioned Directive:

“(28) Considering that all processing of personal data must be carried out lawfully

and loyal with respect to the interested party; which must refer, in particular, to adequate data,

relevant and not excessive in relation to the objectives pursued; that these goals have

to be explicit and legitimate, and must be determined at the time of obtaining the data;

that the objectives of post-obtaining processing cannot be incompatible

with the originally specified objectives.

In short, the moment in which the purposes have to be determined is that of the

collection of data, any type of collection, lacking validity of data collection

with purposes that have not been fixed or determined in a precise way, or so vague or

generic that admitted any purpose. The aim is for the individual to be able to identify the

purposes clearly and precisely, without generating any doubt or difficulty for your

compression.

In addition, the determination of the purposes is necessary to assess whether the treatment

of personal data is "relevant" to the purpose pursued and implies that data should not be collected

personal data that are not necessary for the purpose for which they will be used.

On the other hand, the duty of information and the principle of consent are regulated

in articles 4.1, 5 and 6 of the LOPD:

“Article 5. Right to information in data collection.

1. The interested parties to whom personal data is requested must be previously

expressly, precisely and unequivocally informed:

a) The existence of a file or processing of personal data, the purpose

of the collection of these and of the recipients of the information.

b) Of the mandatory or optional nature of their response to the questions that are

raised.

c) The consequences of obtaining the data or the refusal to provide them.

d) The possibility of exercising the rights of access, rectification, cancellation and opposition.

e) Of the identity and address of the data controller or, where appropriate, of its

representative.

(…)

2. When questionnaires or other forms are used for the collection, they will appear in the

themselves, in clearly legible form, the warnings referred to in the previous section...”.

“Article 6. Consent of the affected party

1. The processing of personal data will require the unequivocal consent of the

affected, unless otherwise provided by law.

2. Consent will not be required when personal data is collected for the

exercise of the functions of the Public Administrations in the field of their

competencies; when they refer to the parties to a contract or pre-contract of a relationship

business, labor or administrative and are necessary for its maintenance or compliance;

when the purpose of data processing is to protect a vital interest of the interested party

under the terms of article 7, section 6, of this Law, or when the data appears in

sources accessible to the public and their treatment is necessary for the satisfaction of the interest

legitimate pursued by the person responsible for the file or by the third party to whom they are communicated

the data, provided that the fundamental rights and freedoms of the user are not violated.

interested.

3. The consent referred to in the article may be revoked when there is cause

justified for it and retroactive effects are not attributed to it.

4. In cases where the consent of the affected party is not necessary for the

processing of personal data, and provided that a law does not provide

Otherwise, the latter may oppose its treatment when there are well-founded and legitimate reasons

related to a specific personal situation. In such a case, the person responsible for the file

will exclude from the treatment the data related to the affected party".

Likewise, the Development Regulation of the LOPD, approved by Royal Decree

1720/2007, of December 21, establishes in its article 10 the assumptions that legitimize the

data processing. Section 1 of this article provides that "The personal data

Personal data may only be processed or transferred if the interested party had

previously given their consent to do so.

Violation of these precepts constitutes a minor infraction in article

44.2.c) (duty to inform) of the LOPD, or serious in articles 44.3.b) (principle of

consent) and c) (principle of proportionality) of the same norm, being able to be

sanctioned with a fine of between 900 and 40,000 euros in the case of minor infractions, and between 40,001 and

300,000 euros for the serious ones.

Article 45.6 of the LOPD admits, exceptionally, the possibility of not agreeing on the

opening of the sanctioning procedure and, instead, warn the responsible subject in order to

that, within the term that the sanctioning body determines, proves the adoption of the measures

corrective measures that in each case are pertinent, provided that the facts are

constituting a minor or serious offense and that the offender had not been sanctioned or

previously noticed.

It is also interesting to highlight the provisions of article 49 of the aforementioned Organic Law,

which grants the sanctioning body the power to require those responsible, in cases

constituting a serious or very serious infringement, the cessation of the illegal use of the data

of a personal nature.

v

In terms similar to Directive 95/46/CE and the LOPD, article 5 of the RGPD is

refers to the principles related to data processing, establishing that the data

will be adequate, pertinent and limited to what is necessary in relation to the purposes

for which they are processed (“data minimization”); and treated lawfully, fairly and

transparent in relation to the interested party (“legality, loyalty and transparency”).

Article 13 of the aforementioned legal text details the “information that must be provided

when the personal data is obtained from the interested party”, at the very moment in which it has

This data collection took place, of which the following stands out:

. The identity and contact details of the person in charge and, where appropriate, of their representative;

. The contact details of the data protection delegate, if any;

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

treatment;

. When the treatment is based on article 6, paragraph 1, letter f), the legitimate interests

of the person in charge or of a third party;

. The period during which the personal data will be kept or, when this is not possible, the

criteria used to determine this term;

. The existence of the right to request access to data from the data controller

related to the interested party, and its rectification or deletion, or the limitation of its treatment, or to oppose the treatment, as well as the right to data portability;

. When the treatment is based on article 6, paragraph 1, letter a), or article 9, paragraph 2, letter a), the existence of the right to withdraw consent at any moment, without affecting the legality of the treatment based on the consent prior to its withdrawal;

. The right to file a claim with a supervisory authority;

. If the interested party is obliged to provide personal data and is informed of the possible consequences of not providing such data;

In relation to the aforementioned principle of transparency, article 11.1 and 2 of the LOPDGDD admits that the affected party be provided with the basic information indicated therein (identity of the person in charge, purpose and exercise of rights) and indicate an address electronically or by any other means that allows easy and immediate access to the remaining information.

On the other hand, articles 6 and 7 of the same RGPD refer, respectively, to the "Legality of the treatment" and the "Conditions for consent".

"Article 6 Legality of the treatment

1. The treatment will only be lawful if at least one of the following conditions is met:

a) the interested party gave his consent for the treatment of his personal data for one or various specific purposes;

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

part 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 data subject or another person

physical;

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 legitimate interests pursued by the

responsible for the treatment or by a third party, provided that said interests are not

prevail the 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 a child.

The provisions of letter f) of the first paragraph shall not apply to the treatment carried out

by public authorities in the exercise of their functions.

2. Member States may maintain or introduce more specific provisions in order to

adapt the application of the rules of this Regulation with regard to the treatment in

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

specific treatment and other measures that guarantee lawful and fair treatment,

including other specific situations of 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 data controller.

The purpose of the treatment must be determined in said legal basis or, as regards

to the treatment referred to in section 1, letter e), will be necessary for the fulfillment of

a mission carried out in the public interest or in the exercise of public powers vested in the

responsible for the treatment. This legal basis may contain specific provisions
to adapt the application of rules of this Regulation, among others: the conditions
general that govern the legality of the treatment by the person in charge; data types
object of treatment; affected stakeholders; the entities to which they can be
communicate personal data and the purposes of such communication; purpose limitation; the
data retention periods, as well as the operations and procedures of the
processing, including measures to ensure fair and lawful processing, such as
relating to other specific situations of treatment under chapter IX. The right to
the Union or the Member States will fulfill an objective of public interest and will be
proportional to the legitimate aim pursued...".

"Article 7 Conditions for consent

1. When the treatment is based on the consent of the interested party, the person in charge must
be able to demonstrate that they consented to the processing of their personal data.

2. If the data subject's consent is given in the context of a written statement that
also refers to other matters, the request for consent will be presented in such a way
clearly distinguishable from other matters, in an intelligible and easily accessible manner and
using clear and simple language. No part of the declaration will be binding.
constitutes an infringement of this Regulation.

3. The interested party will have the right to withdraw their consent at any time. The retreat
of consent will not affect the legality of the treatment based on the prior consent
upon his withdrawal. Before giving their consent, the interested party will be informed of it. it will be so
easy to withdraw consent as to give it.

4. When assessing whether consent has been freely given, it will be taken into account in the greatest extent possible whether, among other things, the performance of a contract, including the provision of a service, is subject to consent to the processing of personal data that are not necessary for the execution of said contract.

The cases in which the treatment refers to special categories of data personal data are regulated in article 9 of the RGPD in the following terms:

"1. The processing of personal data that reveals ethnic origin or racial, political, religious or philosophical convictions, or trade union membership, and the processing of genetic data, biometric data aimed at uniquely identifying to a natural person, data relating to health or data relating to sexual life or sexual orientation of a natural person.

2. Section 1 shall not apply when one of the following circumstances occurs:

a) the interested party gave their explicit consent for the processing of said data for one or more of the specified purposes, except when Union Law or of the Member States provides that the prohibition referred to in paragraph 1 does not it can be raised by the interested party;

(…)".

Failure to comply with the aforementioned precepts constitutes an infringement typified in the article 83.5 of the RGPD, which under the heading "General conditions for the imposition of administrative fines" provides the following:

"Infractions of the following provisions will be sanctioned, in accordance with section

2, with administrative fines of a maximum of EUR 20,000,000 or, in the case of a company, of an amount equivalent to a maximum of 4% of the total annual turnover of the previous financial year, opting for the highest amount:

a) the basic principles for treatment, including the conditions for consent according to articles 5, 6, 7 and 9;

b) the rights of the interested parties pursuant to articles 12 to 22 (…)".

In this regard, the LOPDGDD, in its article 71 establishes that "They constitute infractions the acts and behaviors referred to in sections 4, 5 and 6 of article 83 of Regulation (EU) 2016/679, as well as those that are contrary to this law organic".

For the purposes of the limitation period, article 72 of the LOPDGDD indicates:

"Article 72. Infractions considered very serious.

1. Based on the provisions of article 83.5 of Regulation (EU) 2016/679, considered very serious and will prescribe after three years the infractions that suppose a substantial violation of the articles mentioned therein and, in particular, the following:

a) The processing of personal data violating the principles and guarantees established in the Article 5 of Regulation (EU) 2016/679.

(…)

e) The processing of personal data of the categories referred to in article 9 of the Regulation (EU) 2016/679, without any of the circumstances provided for in said precept and in article 9 of this organic law".

In the event that there is an infringement of the provisions of the RGPD, between the corrective powers available to the Spanish Data Protection Agency, such as control authority, article 58.2 of said Regulation contemplates the following:

"2 Each control authority will have all the following corrective powers indicated next:

(…)

b) sanction any person responsible or in charge of the treatment with a warning when the

treatment operations have violated the provisions of this Regulation;”

(...)

d) order the person responsible or in charge of the treatment that the treatment operations be

comply with the provisions of this Regulation, where appropriate, of a given

manner and within a specified time;

(…)

i) impose an administrative fine under article 83, in addition to or instead of the

measures mentioned in this section, according to the circumstances of each case

particular;".

In relation to the possibility of sanctioning with a warning contemplated in the aforementioned

Article 58.2 b), considers what is stated in Recital 148 of the RGPD:

“In the event of a minor offence, or if the fine likely to be imposed constituted a

disproportionate burden for a natural person, instead of sanction by fine can

impose a warning. However, special attention must be paid to the nature,

gravity and duration of the infraction, to its intentional nature, to the measures taken to

mitigate the damages suffered, the degree of responsibility or any infraction

previous pertinent, to the way in which the supervisory authority had knowledge of the

infraction, to the fulfillment of measures ordered against the person in charge or in charge, to the

adherence to codes of conduct and any other aggravating or mitigating circumstance.”

SAW

The IZENPE entity, constituted as its own medium personified by the Administration
General of the Autonomous Community of Euskadi and the Provincial Councils, was commissioned
of the same for the issuance of means of electronic identification that allow the
citizens and private companies interact telematically with the Basque administration.
To carry out this assignment, IZENPE arranged for two systems (B&K and B&K Q) that
allow identification and electronic signature, formed by a reference number,
password, set of coordinates and electronic signature certificate.
For the development of the aforementioned project, as stated by IZENPE itself, with
date 10/26/2017 signed a collaboration agreement with LANBIDE, by virtue of which this
The latter acts as IZENPE's registration entity for the issuance of means of
digital identification and electronic signature, to facilitate an interoperable system for people
physical users of said employment service. IZENPE has stated that the Department of
Employment and Social Policies decided to implement the system in LANBIDE on an experimental basis
for all workers and users of the service (group close to 300,000 people), to
in order to improve, simplify and make administrative management more efficient, thus responding
to the current needs of society.
Said collaboration agreement was extended and modified to adapt it to the new
regulatory framework on data protection established after the entry into force, on 25
of May 2018, of the RGPD, through the addendum signed on October 15, 2018, in which
the seventh clause on data protection is modified. In its new wording,
specifies that LANBIDE may not use the data for its own purposes, that it will treat it
in accordance with what was determined by IZENPE
For the execution of the agreement, LANBIDE makes its spaces available to IZENPE
physical and the personnel in charge of the tasks of identification and registration of users,
contemplating three phases: a single data collection station initially, an extension

after 10 posts and a third phase (to be executed in the second quarter of 2019), in the

that it is planned to extend the number of registration posts to all the offices of

LANBIDE (43 offices). In this phase it was intended that this means of identification could be

used, by people who voluntarily choose it, for access to the services of

this entity, although IZENPE has indicated that, until the use of the

system (currently in process), will only be tested experimentally.

As stated in the descriptive part, the agreement is framed in Law 39/2015, to

deepen the implementation of electronic administration, and the Regulation (EU)

910/2014. By virtue of this agreement, IZENPE acts in its capacity as service provider

trusted and Lanbide acquires the status of IZENPE registry entity for the

issuance of means of digital identification and electronic signature B&K and B&K Q. in relation

with the natural person users who request means of identification issued by

IZENPE. As such, IZENPE is responsible for the database that will allow the

interoperability of the system, its storage and management.

The aim was to implement an interoperable system that would allow the citizen

interact with the Public Administrations. It is, as defined by IZENPE itself in

their allegations, of a case in which the actions of the entity providing services of

trust is of a general nature and not a singular action that seeks the issuance of a

identification system linked to the exercise of powers of LANBIDE.

From the point of view of personal data protection, IZENPE declares itself

responsible for the treatment (also of the file) and LANBIDE intervenes as manager to

the mere collection and validation of the data and its subsequent sending to IZENPE. This is stated in the formalized documents and in the information provided to the interested parties.

Modifying this position a posteriori would significantly affect the rights of the interested. IZENPE has argued that the "reformulation" of the roles of responsible and in charge of the treatment does not affect the rights of the claimants. However, we we refer here to the damages that this represents for the holders of the personal data in general, that they received clear and specific information about the identity of the responsible (IZENPE) and the way in which they can exercise their rights before said responsible.

For this purpose of altering the condition under which these entities intervene, can be enforced the Resolution of the General Director of LANBIDE dated 30 November 2018, by which it is agreed to "Entrust the company Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe, S.A., as its own personified medium of the General Administration of the Autonomous Community of Euskadi, the provision of services for the implementation in Lanbide of a system that allows the identification of people based on biometric factors", noting that it provides that It corresponds to LANBIDE the definition of the purposes of the treatment and to which a retroactive validity with effect from 01/01/2018.

It should be noted, on the one hand, that this Resolution is not part of the object of the procedure, initiated to analyze the scope of the data collection carried out by LANBIDE by virtue of the aforementioned agreements; and, on the other hand, that it is also Resolution declares IZENPE as data controller, identified in its registration treatment as "management of means of identification based on parameters biometrics".

Also, considering the repeated statements made by IZENPE about the status of data controller attributed to the entity that determines the

purposes of data processing, it is convenient to bear in mind the definition of “responsible

of the treatment” expressed in article 4 of the RGPD, which considers as such not only the one who

defines the purposes, but also the one who enables the means for the treatment, a circumstance that

that is not mentioned by that entity. In this case, it is IZENPE and not LANBIDE who

provides the purposes and means for the treatment, by virtue of its condition as provider of

trust services, referred to above.

Neither can the action of IZENPE be denied as responsible for the treatment of

the data resorting to its nature of its own personified, instrumental means, in relation

with the entities or Public Administrations for which it acts, from the point of view of

the regulation of public sector contracts (article 32 of the LCSP).

Precisely this condition of being responsible for the treatment of IZENPE, and its

nature of a commercial entity, determined the resolution issued by the Basque Agency for

Data Protection for which the reference claims were inadmissible and ordered their

referral to this Spanish Data Protection Agency.

In its allegations to the proposed resolution, IZENPE disregards all the

previous arguments to defend that it cannot be held responsible for the

treatment in any case, especially from the full application of the RGPD. base

this approach in its capacity as a commercial entity with the character of its own medium

personified, which places it in a position of functional dependence on the Administrations

Public companies that carry out “commissions”, from which derives the material impossibility of defining the

purposes of the treatment, not being the owner of the substantive competence that the data serves.

treatment.

He considers that the formalized documents do not determine his status as

responsible, because the distribution of roles of responsible and

in charge of the treatment, going so far as to reproach this Agency for not having carried out any

interpretive effort of such documents to warn ("a sort of lifting of the

veil", says IZENPE) that this company could not be held responsible for the treatment in accordance

with the GDPR. More than an "interpretative effort", what IZENPE is demanding from this

Agency is a modification of the agreed terms and the drawing of conclusions

contrary to the relationship arranged by the IZENPE entity itself.

And he not only wants this Agency to renounce drawing conclusions from relations

formalized by IZENPE in this case, but also the rest of the circumstances

concurrent, with the purpose that the resolution that is issued is based solely on a

conceptual analysis of its condition as a personified medium, as an instrumental entity

which acts on behalf of the Public Administrations on which it depends.

The approach made by IZENPE does not take into account what is established in the aforementioned

article 32 of the LCSP, according to which IZENPE can also act as contracting authority,

as in this case ("3. Section 2 of this article shall also apply in

cases in which the controlled legal person, being a contracting authority, performs a

order to the contracting authority that controls it or to another legal entity controlled, directly or

indirectly, by the same contracting authority, provided that there is no direct participation

of private capital in the legal entity to which the assignment is made").

IZENPE, in the aforementioned allegations, omits something essential for the assessment of the

present case, as is its status as a provider of trusted services according to the

Regulation (EU) 910/2014 (eIDAS), which is at the origin of its creation (IZENPE is

constituted by the Administration of the Autonomous Community of Euskadi and the Provincial Councils

Forales for the development of electronic identification, and its purpose is the issuance and

media management and electronic identification systems for identification,

authentication, signature and/or electronic sealing, to persons or public or private entities).

As such, since 2016 it has been developing the broadcast media project

identification with centralized certificate (in the cloud) for natural persons named

B@k and B@KQ, which seeks to provide citizens with a means of identification in the

telematic relations with the Basque Administrations. Both certificates are issued in a

common repository. When the holder uses the means in question for his identification before

an electronic service, IZENPE, in the event that the authentication is correct, will offer the

body responsible for the service the result of it.

It is an integrated system of eIDAS keys, interoperable, and includes the

creation, verification and validation of identification keys, as well as their preservation.

As explained in the document called “Citizen Certificate Policy”,

published on www.izenpe.eus and notified to the Ministry of Industry, Tourism and Trade,

IZENPE is responsible for verifying the applicant's identity, the application procedure,

issuance and delivery of the means of electronic identification, as well as its revocation and

renewal.

IZENPE is responsible for the collection of data, its storage and the

data processing required by the identification process.

The collaboration agreement signed by IZENPE and LANBIDE is formalized for the

implementation in the latter of these means of electronic identification, within the framework of

Law 39/2015 and Regulation (EU) 910/2014.

7th

The project launched by IZENPE contemplates the collection of data

identification and contact information of the interested parties (surname, name, ID number / Passport,

date of birth, email and mobile phone). Furthermore, to answer

new needs associated with identification systems, the means are completed with

other biometric authentication factors such as fingerprint and/or photograph. as he could

verify the Basque Agency for Data Protection in an inspection carried out on the date

07/06/2018, the process followed by LANBIDE included collecting the fingerprints of the ten

fingers and facial image.

Thus, LANBIDE carries out the following actions, in accordance with the registration system

enabled to collect information:

. Verification of the identity of the interested party through a document validation system

identification presented.

. Obtain the signature of the request for issuance of B@k and B@kQ: a document will be generated

different personalized depending on whether the person has a DNI/NIE and if they already have a B@KQ or

B@K (there will be 3 possible) and the document to be signed by the citizen is printed authorizing the

collection of your biometric data (facial photograph and fingerprint details) by

IZENPE for its relationship with public administrations.

. Collection of identification facial photograph.

. Scanning of fingerprints (the number of them will be parameterizable).

. Register/record the biometric data obtained (photograph and fingerprint) in the system

identity management of IZENPE.

An identification means request form with factors

biometrics, which was subsequently revised to adapt the information it provides,

adapting it to the RGPD. In both forms, the interested parties are informed that they are

means of electronic identification that will allow you to interact with the administrations
Basque and it is detailed that said means of identification are formed by a number of
reference (coinciding with the DNI/NIE/passport of the user and a password), a certificate
non-qualified issued in a centralized repository that will serve for the signature acts
(B@K) or a set of coordinates with 16 positions and a qualified signature certificate
issued in a centralized repository of IZENPE that will serve for the uses of
signature (B@K Q). In both cases, moreover, the means of identification can be
supplemented by other biometric authentication factors such as fingerprint and/or
photograph (only reference to the biometric data that appears in these identity documents)
request).

By signing the corresponding applications, the undersigned declares that he has read and
accepts the Terms and Conditions of use of this means of identification published in
www.izenpe.eus/condicionesuso, and consents to IZENPE processing the data of
personal character referring to the means of identification requested.

On the back of these applications, “Basic information on data protection” is offered.
data”, with the details corresponding to the identity of the person in charge, purpose, legitimacy
(consent of the interested party), recipients and rights, also warning about the
possibility of obtaining more information available on the web “www.izenpe.eus/datos”
access this information and verify that, in the section on the rights of the
concerned, is informed about the possibility of "withdrawing consent").

According to the information provided by IZENPE, the number of users that have been
taken biometric data before the modification of the application forms is 10,378

records, of which 3,624 are prior to the date of entry into force of the RGPD. Behind the modification of the application forms 320 registrations have been made to date 02/15/2019. The total number of registrations as of that date amounts, therefore, to 10,738 users.

In accordance with the foregoing, it is understood that IZENPE is the entity responsible for the collection of data and the subsequent treatment that could entail the use of the means of identification to which the actions refer. In this regard, said entity has declared that it is LANBIDE that defines the purpose of the use of these means and that the last study carried out recommends the reformulation of the roles as responsible and in charge of the data processing, taking into account the condition of IZENPE as its own means of parent administrations. However, it does not clarify how this new reformulation, nor if it is contrary to the information provided to the interested parties about IZENPE's condition as responsible.

On the other hand, it is stated that the legitimate basis for the processing of personal data is the consent of the interested party, provided through the express signature that is obtained through the request forms for means of identification, which also include the Basic information on the protection of personal data. It's about a valid consent, obtained once the transparency requirements have been met established in the applicable regulations.

However, this Agency understands, in relation to the biometric data collected, that the collection of the fingerprint of the ten fingers of the hands violates the principle of "relevance and proportionality" or "minimization of data", regulated in articles 4 of the LOPD and 5 of the RGPD, since the identification measures that are intended to be implemented do not require, to be effective, the collection of the fingerprints of all the fingers of

both hands, which is also not justified due to the intended purpose.

Therefore, the processing of personal data consisting of the collection of fingerprints of the ten fingers of the hands is not proportional to the purpose that justifies the treatment, resulting contrary to the LOPD and the RGPD. This is excessive data collection. when they are not strictly necessary for the intended purpose. In accordance with the principle of minimization, the processing of unnecessary and disproportionate data should be avoided in relation to the intended purposes (limitation of the purpose). And he is responsible for treatment, IZENPE in this case, the one obliged to comply with these principles related to the treatment.

It is true that the information provided refers to the collection of "minutiae fingerprints" and that the number of scanned fingerprints will be configurable. But I do not know provide sufficient details in this regard, nor is it indicated the scope that this represents in relation to the collection of the prints of all the fingers of the hands that came being carried out, as verified by the Basque Data Protection Agency.

Said breach of articles 4.1 of the LOPD and 5 of the RGPD are found classified as a serious infringement in article 44.3 c) of the LOPD ("Treat data of a or use them later in violation of the principles and guarantees established in article 4 of this Law and the provisions that develop it, except when it is constituting a very serious infringement"); and in article 83.5 a) of the RGPD ("Infringements of the following provisions… a) the basic principles for the treatment, including the conditions for consent under articles 5, 6, 7 and 9"), respectively.

Regarding the measures that should be imposed for this non-compliance, In accordance with the provisions of articles 45.6 of the LOPD and 58.2 b) of the RGPD, it is considered appropriate to sanction the aforementioned infraction with a warning.

It is taken into account, on the one hand, that IZENPE has not been sanctioned before and, on the other, that part of the collection of personal data carried out is of a experimental, which has been declared that LANBIDE does not use biometric data for the identification of users as the system is not operational and, mainly, that IZENPE is carrying out a reformulation of the project and has decided to suspend provisionally the processing of biometric data registration for the issuance of media of identification to citizenship while there is no legal coverage, in reference to a standard currently in process, which presumably will provide legal coverage to carry out the identification of citizenship through biometric systems, in the terms established by article 8.2 of the LOPDGDD. In this regard, he has stated to this Agency that since October 26, 2019 this data processing is not being carried out.

IZENPE, however, must clarify the scope of the information offered to the stakeholders about the activation of the identification system. Thus, in the forms of data collection, after the space enabled for the signature of the applicant, is added a section on “Issue and Activation” with the following text: “After identification and signature of the application form, the applicant may initiate the issuance of B@k. The process begins by sending an SMS with the password (which must be changed for security). Finally, Izenpe will generate a non-qualified electronic signature certificate issued in a repository secure centralized

Finally, in response to what was raised by IZENPE in its written arguments to the proposal for a resolution, it is necessary to point out that it is not appropriate to include in this act the

pronouncements that it requests, with a view to the future, on the sanctioning regime applicable to public companies that are their own personified means, which said entity links to the competence that can be attributed to the AVPD and the AEPD in accordance with the provisions of Article 57.1 of the LOPDGDD.

viii

In accordance with the provisions of article 49 of the LOPD, which grants the body sanctioning authority the power to require those responsible, in cases constituting serious or very serious infringement, the cessation of the illicit use of personal data staff; and article 58.2 d) of the RGPD, according to which each control authority may "order the person responsible or in charge of the treatment that the treatment operations be carried out comply with the provisions of this Regulation, where appropriate, of a given manner and within a specified period…"; it is appropriate to require the IZENPE entity so that, within a month, adapt to the personal data protection regulations the treatment operations that it carries out, with the scope expressed in the Fundamentals of Law. Specifically, it is appropriate for IZENPE to cease the illicit use of the data of personal character relating to the fingerprints of the ten fingers of the hands, adjusting this data processing in such a way that the record of a number of fingerprints is kept fingerprints compatible with the principle of data minimization, as long as it is justified properly that number.

It is warned that not meeting the requirements of this organization may be considered as a serious administrative infraction by "not cooperating with the Authority of control" before the requests made, being able to be valued such conduct at the time of the opening of an administrative sanctioning procedure with a pecuniary fine.

Therefore, in accordance with the applicable legislation and having assessed the criteria for graduation of sanctions whose existence has been proven,

the Director of the Spanish Data Protection Agency RESOLVES:

FIRST: IMPOSE EMPRESA DE CERTIFICACION Y SERVICIOS IZENPE, S.A., with

NIF A01337260, a sanction of warning, for an infraction of articles 4.1 of the

LOPD and 5 of the RGPD, typified in articles 44.3 c) of the LOPD and 83.5 a) of the RGPD,

respectively.

SECOND: REQUEST the entity CERTIFICATION AND SERVICES COMPANY

IZENPE, S.A., so that within one month, counted from the notification of this act,

adapt to the personal data protection regulations the treatment operations that

performs, with the scope expressed in the Legal Basis VIII. Specifically, it is required

that IZENPE cease the illicit use of personal data related to the

fingerprints of the ten fingers of the hands, adjusting this data treatment of

such that a record of a number of fingerprints compatible with the

principle of data minimization, provided that this number is duly justified.

THIRD: NOTIFY this resolution to the entity CERTIFICATION COMPANY

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es

45/45

AND SERVICES IZENPE, S.A.

In accordance with the provisions of article 50 of the LOPDGDD, this

Resolution will be made public once it has been notified to the interested parties.

Against this resolution, which puts an end to the administrative procedure in accordance with art. 48.6 of the

LOPDGDD, and in accordance with the provisions of article 123 of the LPACAP, the interested parties

may optionally file an appeal for reconsideration before the Director of the Agency

Spanish Data Protection Authority within a month from the day following the

notification of this resolution or directly contentious-administrative appeal before the Chamber

of the Contentious-administrative of the National High Court, in accordance with the provisions of the article 25 and in section 5 of the fourth additional provision of Law 29/1998, of 13 July, regulatory of the Contentious-administrative Jurisdiction, in the term of two months to count from the day following the notification of this act, as provided in article 46.1 of the aforementioned Law.

Finally, it is pointed out that in accordance with the provisions of art. 90.3 a) of the LPACAP, may provisionally suspend the firm resolution in administrative proceedings if the interested party states its intention to file a contentious-administrative appeal. If this is the case, The interested party must formally communicate this fact in writing addressed to the Agency Spanish Data Protection, presenting it through the Electronic Registry of the Agency [https://sedeagpd.gob.es/sede-electronica-web/], or through one of the remaining records provided for in art. 16.4 of the aforementioned Law 39/2015, of October 1. You must also transfer to the Agency the documentation that proves the effective filing of the contentious-administrative appeal. If the Agency were not aware of the filing of the contentious-administrative appeal within two months from the day following the notification of this resolution, it would end the suspension precautionary

Sea Spain Marti

Director of the Spanish Data Protection Agency

C/ Jorge Juan, 6

28001 – Madrid

www.aepd.es

sedeagpd.gob.es