No. 294

DISCLAIMER - Automatic translation: This document is an unofficial translation to facilitate the understanding of the university regulatory framework in Spain. The University is not responsible for it. The official version of this document is available in Spanish at the following link: BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

NOTA ACLARATORIA – Traducción automática: *El presente documento es una traducción no oficial para facilitar a los interesados la comprensión del marco regulatorio universitario en España. La Universidad no se hace responsable de la misma. Puede consultar en castellano la versión oficial del presente documento en el siguiente* enlace: BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

I. GENERAL PROVISIONS

HEAD OF STATE

16673 *Organic Law 3/2018, of December 5, on Personal Data Protection and guarantee of digital rights.*

FELIPE VI

KING OF SPAIN

To all who see and understand this document.
Be it known: That the Cortes Generales have approved and I come to sanction the following organic law.

İNDICE

PREAMBLE

The protection of natural persons in relation to the processing of personal data is a fundamental right protected by article 18.4 of the Spanish Constitution. Thus, our Constitution was a pioneer in the recognition of the fundamental right to the protection of personal data when it provided that "the ley shall limit the use of information technology to ensure the honor and personal and family privacy

of citizens and the full exercise of their rights". It thus echoed the work developed since the end of the 1960s in the Council of Europe and the few legal provisions adopted in neighboring countries.

The Constitutional Court pointed out in its Ruling 94/1998, of May 4, 1998, that we are dealing with a fundamental right to data protection, which guarantees the individual control over his or her data, any personal data, and over their use and destination, in order to avoid unlawful trafficking of such data or data that is harmful to the dignity and rights of those affected; in this way, the right to data protection is configured as a power of the citizen to oppose the use of certain personal data for purposes other than that which justified their collection. For its part, Ruling 292/2000, of November 30, 2000, considers it as an autonomous and independent right consisting of a power of disposal and control over personal data that empowers the individual to decide which of those data to provide to a third party, whether the State or a private individual, or which may be collected by this third party, and which also allows the individual to know who possesses such personal data and for what purpose, being able to oppose such possession or use.

At the legislative level, the concretion and development of the fundamental right to protection of natural persons in relation to the processing of personal data took place in its origins through the approval of Organic Law 5/1992, of October 29, 1992, regulating the automated processing of personal data, known as LORTAD. Organic Law 5/1992 was replaced by Organic Law 15/1999, of December 5, 1999, on the protection of personal data, in order to transpose into Spanish law Directive 95/46/EC of the European Parliament and of the Council, of October 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This organic law represented a second milestone in the evolution of the regulation of the fundamental right to data protection in Spain and was complemented by an increasingly abundant jurisprudence from the bodies of the contentious-administrative jurisdiction.

It is also included in Article 8 of the Charter of Fundamental Rights of the European Union and in Article 16.1 of the Treaty on the Functioning of the European Union. Previously, at European level, the aforementioned Directive 95/46/EC had been adopted, the purpose of which was to ensure that the guarantee of the right to the protection of personal data did not constitute an obstacle to the free movement of data within the Union, thus establishing a common area of guarantee of the right which, at the same time, would ensure that in the event of international transfer of data, their processing in the country of destination would be protected by safeguards adequate to those provided for in the directive itself.

In the last few years of the last decade, there was an intensification of efforts to achieve a more uniform regulation of the fundamental right to data protection within the framework of an increasingly globalized society. Thus, proposals for the reform of the current framework were adopted in various international bodies. In this context, on November 4, 2010, the Commission launched its Communication entitled "A Global Approach to Data Protection in the European Union", which is the seed of the subsequent reform of the European Union framework. At the same time, the Court of Justice of the European Union has been adopting over the last few years a case law that is fundamental in its interpretation.

The latest milestone in this evolution took place with the adoption of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of their personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), as well as Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by the competent authorities.

for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data and repealing Council Framework Decision 2008/977/JHA.

The General Data Protection Regulation aims with its direct effectiveness to overcome the obstacles that prevented the harmonizing purpose of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The transposition of the directive by the Member States has resulted in a regulatory patchwork with irregular profiles throughout the European Union, which has ultimately led to appreciable differences in the protection of citizens' rights.

It also takes into account new circumstances, mainly the increase in cross-border flows of personal data as a result of the functioning of the internal market, the challenges posed by rapid technological evolution and globalization, which has made personal data the fundamental resource of the information society. The centrality of personal information has positive aspects, because it enables new and better services, products or scientific findings. But it also has risks, because information on individuals is multiplying exponentially, is more accessible to more actors, and is increasingly easy to process, while it is more difficult to control its destination and use.

The General Data Protection Regulation revises the legal basis of the European data protection model beyond a mere update of the existing rules. It reinforces legal certainty and transparency while allowing its rules to be specified or restricted by the law of the Member States to the extent necessary for reasons of consistency and to make the national provisions comprehensible to those to whom they are addressed. Thus, the General Data Protection Regulation contains a large number of authorizations, if not impositions, on the Member States, in order to regulate certain matters, even allowing in its Recital 8, and in contrast to what is a general principle of European Union law, that when its rules must be specified, interpreted or, exceptionally, restricted by the law of the Member States, the latter have the possibility of incorporating into national law provisions specifically contained in the regulation, to the extent necessary for reasons of consistency and comprehensibility.

At this point it should be emphasized that not all intervention of domestic law in the areas covered by European regulations is excluded. On the contrary, such intervention may be appropriate, or even necessary, both for the purification of the national legal system and for the development or supplementing of the regulation in question. Thus, the principle of legal certainty, in its positive aspect, obliges the Member States to integrate the European legal system into their domestic law in a sufficiently clear and public manner to enable it to be fully understood both by legal operators and by the citizens themselves, while, in its negative aspect, it implies the obligation for such States to eliminate situations of uncertainty deriving from the existence of rules in national law that are incompatible with European law. From this second aspect derives the consequent obligation to purify the legal system. In short, the principle of legal certainty requires that domestic legislation that is incompatible with European Union law be definitively eliminated "by means of binding domestic provisions having the same legal value as the domestic provisions to be amended" (Judgments of the Court of Justice of 23 February 2006, Commission v. Spain; of 13 July 2000, Commission v. France; and of 15 October 1986, Commission v. Italy). Finally, regulations, despite their direct applicability, may in practice require other complementary internal rules in order to be fully implemented.

effective application. In this sense, rather than incorporation, it would be more appropriate to talk about "development" or complement of European Union law.

The adaptation to the General Data Protection Regulation, which will be applicable as of May 25, 2018, as established in its article 99, requires, in short, the drafting of a new organic law to replace the current one. In this work, the principles of good regulation have been preserved, as it is a necessary rule for the adaptation of the Spanish legal system to the aforementioned European provision and proportional to this objective, its ultimate reason being to provide legal certainty.

IV

The Internet, on the other hand, has become an omnipresent reality in both our personal and collective lives. A large part of our professional, economic and private activity takes place on the Net and is of fundamental importance both for human communication and for the development of our life in society. As early as the 1990s, and aware of the impact that the Internet was going to have on our lives, the pioneers of the Net proposed the drafting of a Declaration of the Rights of Man and the Citizen on the Internet.

Today we identify quite clearly the risks and opportunities that the world of networks offers to citizens. It is up to the public authorities to promote policies that make the rights of citizenship on the Internet effective, promoting the equality of citizens and the groups they belong to in order to make possible the full exercise of fundamental rights in the digital reality. The digital transformation of our society is already a reality in our present and future development both socially and economically. In this context, countries in our environment have already approved regulations that reinforce the digital rights of citizens.

The constituents of 1978 already sensed the enormous impact that technological advances would have on our society and, in particular, on the enjoyment of fundamental rights. A desirable future reform of the Constitution should include among its priorities the updating of the Constitution to the digital era and, specifically, the elevation to constitutional rank of a new generation of digital rights. However, until this challenge is met, the legislator must address the recognition of a system for guaranteeing digital rights which, unequivocally, is anchored in the mandate imposed by the fourth paragraph of article 18 of the Spanish Constitution and which, in some cases, have already been outlined by ordinary, constitutional and European jurisprudence.

V

This organic law consists of ninety-seven articles structured in ten titles, twenty-two additional provisions, six transitory provisions, one derogatory provision and sixteen final provisions.

Title I, relating to general provisions, begins by regulating the purpose of the Organic Law, which is, as indicated above, twofold. Thus, in the first place, it aims to achieve the adaptation of the Spanish legal system to Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, General Data Protection Regulation, and to complete its provisions. In turn, it establishes that the fundamental right of natural persons to the protection of personal data, protected by Article 18.4 of the Constitution, shall be exercised in accordance with the provisions of Regulation (EU) 2016/679 and this Organic Law. The autonomous communities have powers of regulatory development and enforcement of the fundamental right to the protection of personal data in their sphere of activity and the autonomous data protection authorities that are created are responsible for contributing to guarantee this fundamental right of citizens. Secondly, it is also the purpose of the Law to guarantee the digital rights of citizens, pursuant to the provisions of article 18.4 of the Constitution.

The novel regulation of data referring to deceased persons stands out, since, after excluding their processing from the scope of application of the ley, it allows persons linked to the deceased for family or de facto reasons or their heirs to request access to them, as well as their rectification or deletion, if necessary, subject to the instructions of the deceased. It also excludes from the scope of application the processing governed by specific provisions, in reference, among others, to the regulations transposing the aforementioned Directive (EU) 2016/680, with the fourth transitory provision providing for the application to such processing of Organic Law 15/1999, of December 13, until the aforementioned regulations are approved.

Title II, "Data protection principles", establishes that for the purposes of Regulation (EU) 2016/679, the inaccuracy of the data obtained directly from the data subject shall not be imputable to the controller, provided that the controller has taken all reasonable steps to ensure that the data is erased or rectified without delay, when it has received the data from another data controller by virtue of the exercise by the data subject of the right to portability, or when the data controller has obtained them from an intermediary or broker when the rules applicable to the sector of activity to which the data controller belongs establish the possibility of the intervention of an intermediary or broker or when the data have been obtained from a public register. It also expressly includes the duty of confidentiality, the processing of data covered by the Law, the special categories of data and the processing of data of a criminal nature, and specifically refers to consent, which must come from a declaration or a clear affirmative action by the data subject, excluding what used to be known as "tacit consent", it is stated that the consent of the data subject for a plurality of purposes must be specifically and unequivocally stated that it is given for all of them, and the age at which minors may give their consent is maintained at fourteen years of age.

It also regulates the possible legal authorizations for processing based on compliance with a legal obligation required of the controller, under the terms provided for in Regulation (EU) 2016/679, when so provided by a rule of European Union law or an ley, which may determine the general conditions of the processing and the types of data subject to it as well as the transfers that may proceed as a result of compliance with the legal obligation, This is the case, for example, This is the case, for example, of the databases regulated by Law and managed by public authorities that respond to specific objectives of risk and solvency control, supervision and inspection of the type of the Central Credit Register of the Bank of Spain regulated by Law 44/2002, of November 22nd, on Financial System Reform Measures, or data, documents and information of a reserved nature held by the Directorate General of Insurance and Pension Funds in accordance with the provisions of Law 20/2015, of July 14, on the regulation, supervision and solvency of insurance and reinsurance entities.

Special conditions may also be imposed on the processing, such as the adoption of additional security measures or others, when it derives from the exercise of public powers or the fulfillment of a legal obligation and may only be considered to be based on the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the controller, in the terms provided for in the European regulation, when it derives from a competence conferred by the law. And the prohibition on consenting to processing with the main purpose of storing identifying information of certain categories of specially protected data is maintained, which does not prevent them from being processed in the other cases provided for in Regulation (EU) 2016/679. Thus, for example, the provision of consent will not cover the creation of "blacklists" of trade unionists, although trade union membership data may be processed by the employer to enable the exercise of workers' rights under Article 9(2)(b) of Regulation (EU) 2016/679 or by the trade unions themselves under the terms of Article 9(2)(d) of the same European regulation.

Also in relation to the processing of special categories of data, Article 9.2 enshrines the principle of reservation of ley for its authorization in the cases provided for in Regulation (EU) 2016/679. This provision not only reaches the provisions that could be adopted in the future, but also allows to leave the various legal authorizations currently in existence untouched, as specifically indicated, with respect to health and insurance legislation, in the seventeenth additional provision. The General Data Protection Regulation does not affect these authorizations, which remain fully in force, even allowing for an extensive interpretation of them, as is the case, in particular, with regard to the scope of the data subject's consent or the use of his or her data without consent in the field of biomedical research. To this end, paragraph 2 of the seventeenth additional provision introduces a series of provisions aimed at guaranteeing the adequate development of research in the field of health, and in particular biomedical research, weighing up the unquestionable benefits it brings to society with the due guarantees of the fundamental right to data protection.

Title III, dedicated to the rights of individuals, adapts to Spanish law the principle of transparency in the processing of the European regulation, which regulates the right of data subjects to be informed about the processing and includes the so called
The "layered information" already generally accepted in areas such as video surveillance or the installation of mass data storage devices (such as "cookies"), providing the affected party with the basic information, but indicating an e-mail address or other means that allows easy and immediate access to the remaining information.

Use is made in this Title of the empowerment allowed by Recital 8 of Regulation (EU) 2016/679 to supplement its regime, ensuring the appropriate systematic structure of the text. Next, the Organic Law provides for the rights of access, rectification, erasure, opposition, right to limitation of processing and right to portability.

Title IV contains "Provisions applicable to specific processing operations", incorporating a series of cases that should by no means be considered exhaustive of all lawful processing operations. These include, in the first place, those in respect of which the legislator establishes a "iuris tantum" presumption of the prevalence of the legitimate interest of the data controller when they are carried out in compliance with a series of requirements, which does not exclude the lawfulness of this type of processing when the conditions laid down in the text are not strictly met, although in this case the data controller must carry out the legally required weighing up, since the prevalence of his legitimate interest is not presumed. Along with these cases, others are included, such as video surveillance, advertising exclusion files or internal complaints systems in which the lawfulness of the processing stems from the existence of a public interest, in the terms established in Article 6.1.e) of Regulation (EU) 2016/679. Finally, reference is made in this Title to the lawfulness of other processing regulated in Chapter IX of the regulation, such as those related to the statistical function or for archiving purposes of general interest. In any case, the fact that the legislator refers to the lawfulness of processing does not detract from the obligation of controllers to adopt all the measures of active responsibility established in Chapter IV of the European regulation and in Title V of this Organic Law.

Title V refers to the controller and the processor. It should be noted that the main novelty of Regulation (EU) 2016/679 is the evolution from a model based primarily on compliance control to one based on the principle of active responsibility, which requires a prior assessment by the controller or processor of the risk that could be generated by the processing of personal data in order to, based on this assessment, adopt the appropriate measures. In order to clarify these new features, the Organic Law maintains the same name of Chapter IV of the Regulation, dividing the articles into four chapters dedicated, respectively, to the general measures of active responsibility, to the regime of the data processor, to the figure of the data protection officer and to

self-regulation and certification mechanisms. The figure of the data protection officer acquires a prominent importance in Regulation (EU) 2016/679 and this is reflected in the Organic Law, which is based on the principle that he/she can have a mandatory or voluntary character, be integrated or not in the organization of the responsible or in charge and be both a natural person and a legal person. The designation of the data protection officer must be communicated to the competent data protection authority. The Spanish Data Protection Agency will keep a public and updated list of data protection officers, accessible to any person. Knowledge of the subject may be accredited by means of certification schemes. Likewise, he/she may not be removed, except in cases of fraud or serious negligence. It should be noted that the data protection officer allows setting up a means for the amicable resolution of claims, since the data subject may submit to him/her the claim that is not attended to by the data controller or data processor.

Title VI, on international data transfers, proceeds to the adaptation of the provisions of Regulation (EU) 2016/679 and refers to the specialties related to the procedures through which the data protection authorities may approve contractual models or binding corporate rules, assumptions of authorization of a certain transfer, or prior information.

Title VII is dedicated to the data protection authorities, which, following the mandate of Regulation (EU) 2016/679, are to be established by national law. Maintaining the scheme that had been included in its regulatory background, the organic law regulates the regime of the Spanish Data Protection Agency and reflects the existence of the autonomous data protection authorities and the necessary cooperation between the supervisory authorities. The Spanish Data Protection Agency is configured as an independent administrative authority under Law 40/2015, of 1 October, on the Legal Regime of the Public Sector, which is related to the Government through the Ministry of Justice.

Title VIII regulates the "Procedures in case of possible breach of data protection regulations". Regulation (EU) 2016/679 establishes a novel and complex system, evolving towards a "one-stop shop" model in which there is a lead supervisory authority and other authorities concerned. It also establishes a cooperation procedure between Member State authorities and, in case of discrepancy, provides for a binding decision by the European Data Protection Board. Consequently, prior to any procedure, it will be necessary to determine whether or not the processing is of a cross-border nature and, if so, which data protection authority is to be considered the lead data protection authority.

The regulation is limited to delimiting the legal regime; the initiation of proceedings, with the Spanish Data Protection Agency being able to refer the claim to the data protection officer or to the bodies or entities responsible for the extrajudicial resolution of conflicts in accordance with the provisions of a code of conduct; the rejection of claims; preliminary investigation actions; provisional measures, including the order to block the data; and the time limit for processing the proceedings and, if appropriate, their suspension. The special features of the procedure are referred to the regulatory development.

Title IX, which contemplates the sanctioning regime, starts from the fact that Regulation (EU) 2016/679 establishes a system of sanctions or corrective actions that allows a wide margin of appreciation. Within this framework, the Organic Law proceeds to describe the typical conducts, establishing the distinction between very serious, serious and minor infringements, taking into consideration the differentiation that the General Data Protection Regulation establishes when setting the amount of penalties. The categorization of the infringements is introduced for the sole purpose of determining the statute of limitations, the description of the typical conducts having as its sole purpose the exemplary enumeration of some of the punishable acts that must be understood to be included within the general types established in the European regulation. The Organic Law regulates the cases of interruption of the statute of limitations on the basis of the constitutional requirement of the

knowledge of the facts imputed to the person, but taking into account the problems arising from the procedures established in the European regulation, depending on whether the procedure is handled exclusively by the Spanish Data Protection Agency or whether the coordinated procedure of Article 60 of the General Data Protection Regulation is used.

Regulation (EU) 2016/679 establishes wide margins for the determination of the amount of penalties. The Organic Law takes advantage of the residual clause of Article 83.2 of the European standard, referring to aggravating or mitigating factors, to clarify that the elements to be taken into account may include those that already appeared in Article 45.4 and 5 of Organic Law 15/1999, and which are known to legal operators.

Finally, Title X of this Law undertakes the task of recognizing and guaranteeing a list of digital rights of citizens in accordance with the mandate established in the Constitution. In particular, the rights and freedoms applicable to the Internet environment, such as net neutrality and universal access or the rights to digital security and education, as well as the rights to be forgotten, to portability and to a digital will, are regulated. The recognition of the right to digital disconnection within the framework of the right to privacy in the use of digital devices in the workplace and the protection of minors on the Internet occupies a relevant place. Finally, it is noteworthy the guarantee of freedom of expression and the right to clarification of information in digital media.

The additional provisions refer to issues such as security measures in the public sector, data protection and transparency and access to public information, calculation of deadlines, judicial authorization for international data transfers, protection against abusive practices that may be developed by certain operators, or the processing of health data, among others.

Pursuant to the fourteenth additional provision, the regulations relating to the exceptions and limitations in the exercise of the rights that had entered into force prior to the date of application of the European regulation, and in particular articles 23 and 24 of Organic Law 15/1999, of December 13, on the Protection of Personal Data, will remain in force until such time as they are expressly amended, replaced or repealed. The survival of this regulation implies the continuity of the exceptions and limitations contained therein until it is reformed or repealed, albeit referring to the rights as regulated in Regulation (EU) 2016/679 and in this Organic Law. Thus, for example, by virtue of the aforementioned additional provision, the tax administrations responsible for the data files with tax implications referred to in Article 95 of Law 58/2003, of December 17, General Tax Law, may, in relation to such data, deny the exercise of the rights referred to in Articles 15 to 22 of Regulation (EU) 2016/679, when the same hinders the administrative actions aimed at ensuring compliance with tax obligations and, in any case, when the data subject is being subject to inspection actions.

The transitional provisions are dedicated, among other issues, to the statute of the Spanish Data Protection Agency, the transitional regime of the procedures or the processing subject to Directive (EU) 2016/680. A repealing provision is included, followed by the final provisions on the precepts with the character of ordinary law, the competence title and the entry into force.

It also introduces the necessary amendments to Law 1/2000, of January 7, on Civil Proceedings and Law 29/1998, of July 13, regulating the Contentious-Administrative Jurisdiction, Organic Law, 6/1985, of July 1, on the Judiciary, Law 19/2013, of December 9, on Transparency, access to public information and good governance, Organic Law 5/1985, of June 19, 1985, on the General Electoral Regime, Law 14/1986, of April 25, 1986, on General Health, Law 41/2002, of November 14, 2002, basic law regulating patient autonomy and rights and obligations in the field of health, and the Law on the protection of patients' rights and obligations, of November 14, 2002, on the protection of patients' rights and obligations in the field of health, of November 14, 2002, on the protection of patients' rights and obligations in the field of health.

of information and clinical documentation and Law 39/2015, of October 1, of the Common Administrative Procedure of Public Administrations.

Finally, and in relation to the guarantee of digital rights, amendments are also introduced in the Organic Law 2/2006, of May 3, on Education, the Organic Law 6/2001, of December 21, on Universities, as well as in the Revised Text of the Workers' Statute Law and in the Revised Text of the Basic Statute of the Public Employee.

TITLE I

General Provisions

Article 1. *Object of the Law.*

The purpose of this organic law is:

a) To adapt the Spanish legal system to Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of their personal data and on the free movement of such data, and to complete its provisions.

The fundamental right of individuals to the protection of personal data, protected by Article 18.4 of the Constitution, shall be exercised in accordance with the provisions of Regulation (EU) 2016/679 and this Organic Law.

b) Guarantee the digital rights of citizens in accordance with the mandate established in Article 18.4 of the Constitution.

Scope of application of Titles I to IX and addenda 89 to 94.

1. The provisions of Titles I to IX and Articles 89 to 94 of this Organic Law apply to any fully or partially automated processing of personal data, as well as to the non-automated processing of personal data contained or intended to be included in a file.

2. This organic law shall not apply:

a) To the processing excluded from the scope of application of the General Data Protection Regulation by its article 2.2, without prejudice to the provisions of paragraphs 3 and 4 of this article.

b) To the processing of data of deceased persons, without prejudice to the provisions of Article 3.

c) Treatments subject to regulations on the protection of classified materials.

3. Processing operations to which Regulation (EU) 2016/679 is not directly applicable because it affects activities not included in the scope of application of European Union Law, shall be governed by the provisions of their specific legislation, if any, and supplementarily by the provisions of the aforementioned regulation and this Organic Law. This situation includes, among others, the treatments carried out under the protection of the organic legislation of the general electoral regime, the treatments carried out in the field of penitentiary institutions and the treatments derived from the Civil Registry, the Property and Mercantile Registries.

4. The processing of data carried out on the occasion of the processing by the judicial bodies of the processes for which they are competent, as well as that carried out within the management of the Judicial Office, shall be governed by the provisions of Regulation (EU) 2016/679 and this Organic Law, without prejudice to the provisions of Organic Law 6/1985, of 1 July, on the Judiciary, which are applicable to it.

Article 3. *Data of deceased persons.*

1. Persons related to the deceased for family or de facto reasons, as well as their heirs, may contact the data controller or data processor to request access to their personal data and, where appropriate, their rectification or erasure.

As an exception, the persons referred to in the preceding paragraph may not access the data of the deceased, nor request its rectification or deletion, when the deceased had expressly forbidden it or it is so established by law. Said prohibition shall not affect the right of the heirs to access the data of the deceased's estate.

2. The persons or institutions that the deceased had expressly designated for this purpose may also request, in accordance with the instructions received, access to the deceased's personal data and, where appropriate, its rectification or deletion.

A Royal Decree will establish the requirements and conditions for accrediting the validity and validity of these mandates and instructions and, if applicable, their registration.

3. In the event of the death of minors, these powers may also be exercised by their legal representatives or, within the framework of its competencies, by the Public Prosecutor's Office, which may act ex officio or at the request of any interested individual or legal entity.

In the event of death of persons with disabilities, these powers may also be exercised, in addition to those mentioned in the preceding paragraph, by those who have been designated for the exercise of support functions, if such powers are understood to be included in the support measures provided by the designated person.

TITLE II

Data protection principles

Article 4. *Accuracy of data.*

1. In accordance with Article 5(1)(d) of Regulation (EU) 2016/679 the data shall be accurate and, if necessary, updated.

2. For the purposes provided for in Article 5(1)(d) of Regulation (EU) 2016/679, the controller shall not be held liable, provided that the controller has taken all reasonable steps to have the personal data deleted or rectified without delay, for inaccurate personal data, with respect to the purposes for which they are processed, when the data inaccurate:

a) They would have been obtained by the responsible party directly from the affected party.

b) Had been obtained by the data controller from a mediator or intermediary in the event that the rules applicable to the sector of activity to which the data controller belongs provide for the possibility of intervention of an intermediary or mediator who collects the data of the data subjects on their own behalf for transmission to the data controller. The mediator or intermediary shall assume the responsibilities that may arise in the event of communication to the controller of data that do not correspond to those provided by the data subject.

c) Were subject to processing by the controller because they were received from another controller by virtue of the exercise by the data subject of the right to portability in accordance with Article 20 of Regulation (EU) 2016/679 and the provisions of this Organic Law.

d) Were obtained from a public record by the responsible party.

Article 5. *Duty of confidentiality.*

1. Data controllers and processors as well as all persons involved at any stage of data processing shall be subject to the duty of confidentiality referred to in Article 5(1)(f) of Regulation (EU) 2016/679.

2. The general obligation indicated in the preceding paragraph shall be complementary to the duties of professional secrecy in accordance with the applicable regulations.

3. The obligations set forth in the preceding paragraphs shall be maintained even if the relationship between the obligor and the data controller or data processor has ended.

Article 6. *Processing based on the consent of the data subject.*

1. In accordance with the provisions of Article 4.11 of Regulation (EU) 2016/679, consent of the data subject means any freely given, specific, informed and unambiguous expression of will by which the data subject agrees, either by a statement or by a clear affirmative action, to the processing of personal data concerning him or her.

2. When the processing of data is intended to be based on the consent of the data subject for a plurality of purposes, it shall be necessary to specifically and unequivocally state that such consent is given for all of them.

3. The execution of the contract may not be made conditional upon the data subject's consent to the processing of personal data for purposes unrelated to the maintenance, development or control of the contractual relationship.

Article 7. *Consent of minors.*

1. The processing of a minor's personal data may only be based on his or her consent when he or she is over fourteen years of age.

Exceptions are those cases in which the Law requires the assistance of the holders of parental authority or guardianship for the execution of the act or legal transaction in the context of which the consent for the processing is sought.

2. The processing of data of minors under fourteen years of age, based on consent, shall only be lawful if the consent of the holder of parental authority or guardianship is given, to the extent determined by the holders of parental authority or guardianship.

Article 8. *Processing of data due to legal obligation, public interest or exercise of public powers.*

1. The processing of personal data may only be considered to be based on compliance with a legal obligation incumbent on the controller, in the terms provided for in Article 6.1.c) of Regulation (EU) 2016/679, when so provided by a rule of European Union law or a rule with the rank of ley, which may determine the general conditions of the processing and the types of data subject to it as well as the transfers that proceed as a result of the fulfillment of the legal obligation. Such a rule may also impose special conditions for processing, such as the adoption of additional security measures or other measures provided for in Chapter IV of Regulation (EU) 2016/679.

2. The processing of personal data may only be considered to be based on the performance of a task carried out in the public interest or in the exercise of public powers conferred on the controller, in the terms provided for in Article 6.1 e) of Regulation (EU) 2016/679, when it derives from a competence conferred by a regulation with the rank of ley.

Article 9. *Special categories of data.*

1. For the purposes of Article 9(2)(a) of Regulation (EU) 2016/679, in order to avoid discriminatory situations, the consent of the data subject alone shall not be sufficient to lift the prohibition on the processing of data whose primary purpose is to identify his or her ideology, trade union membership, religion, sexual orientation, beliefs or racial or ethnic origin.

The provisions of the preceding paragraph shall not prevent the processing of such data under the other cases referred to in Article 9.2 of Regulation (EU) 2016/679, where appropriate.

2. The processing of data referred to in letters g), h) and i) of Article 9.2 of Regulation (EU) 2016/679 based on Spanish law must be covered by a regulation with the rank of ley, which may establish additional requirements relating to their security and confidentiality.

In particular, this rule may cover the processing of data in the field of health when required for the management of public and private health and social care systems and services, or for the performance of an insurance contract to which the data subject is a party.

Article 10. *Processing of data of a criminal nature.*

1. The processing of personal data relating to criminal convictions and offences, as well as to proceedings and related precautionary and security measures, for purposes other than the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, may only be carried out when it is covered by a rule of Union law, by this Organic Law or by other rules of law.

2. The complete registration of data referring to criminal convictions and offenses, as well as to proceedings and related precautionary and security measures referred to in Article 10 of Regulation (EU) 2016/679, may be carried out in accordance with the provisions of the regulation on the System of administrative records to support the Administration of Justice.

3. Apart from the cases indicated in the previous paragraphs, the processing of data referring to criminal convictions and offenses, as well as related precautionary and security procedures and measures will only be possible when they are carried out by lawyers and attorneys and their purpose is to collect the information provided by their clients for the exercise of their functions.

TITLE III

Rights of individuals

CHAPTER I

Transparency and information

Article 11. *Transparency and information to the affected party.*

1. Where personal data are obtained from the data subject the controller may comply with the duty of information set forth in Article 13 of Regulation (EU) 2016/679 by providing the data subject with the basic information referred to in the following paragraph and indicating an e-mail address or other means that allows easy and immediate access to the remaining information.

2. The basic information referred to in the previous paragraph shall contain, at least:

a) The identity of the data controller and its representative, if applicable.
b) The purpose of the treatment.

c) The possibility to exercise the rights set out in Articles 15 to 22 of Regulation (EU) 2016/679.

If the data obtained from the data subject is to be processed for profiling purposes, the basic information shall also include this circumstance. In this case, the data subject shall be informed of his or her right to object to the adoption of automated individual decisions that produce legal effects on him or her or significantly affect him or her in a similar way, when this right is present in accordance with the provisions of Article 22 of Regulation (EU) 2016/679.

3. When the personal data have not been obtained from the data subject, the data controller may comply with the duty of information established in Article 14 of Regulation (EU) 2016/679 by providing the data subject with the basic information indicated in the previous paragraph, indicating an e-mail address or other means that allows easy and immediate access to the remaining information.

In these cases, the basic information shall also include:

a) The categories of data to be processed.
b) The sources from which the data originated.

CHAPTER II

Exercise of rights

Article 12. *General provisions on the exercise of rights.*

1. The rights recognized in Articles 15 to 22 of Regulation (EU) 2016/679, may be exercised directly or through a legal representative or volunteer.

2. The data controller shall be obliged to inform the data subject of the means at his disposal to exercise the rights to which he is entitled. The means must be easily accessible to the data subject. The exercise of the right may not be refused on the sole ground that the data subject chooses another means.

3. The person in charge may process, on behalf of the data controller, requests for the exercise of their rights made by the data subjects if so established in the contract or legal act that binds them.

4. Proof of compliance with the duty to respond to a request by the data subject to exercise his or her rights shall be provided by the data controller.

5. Where the laws applicable to certain processing operations establish a special regime affecting the exercise of the rights provided for in Chapter III of Regulation (EU) 2016/679, the provisions of those laws shall apply.

6. In any case, the holders of parental authority may exercise the rights of access, rectification, cancellation, opposition or any other rights that may correspond to them in the context of the present Organic Law, in the name and on behalf of minors under fourteen years of age.

7. The actions carried out by the controller to deal with requests to exercise these rights shall be free of charge, without prejudice to the provisions of Articles 12.5 and 15.3 of Regulation (EU) 2016/679 and Article 13(3) and (4) of this Organic Law.

Article 13. *Right of access.*

1. The data subject's right of access shall be exercised in accordance with the provisions of Article 15 of Regulation (EU) 2016/679.

Where the controller processes a large amount of data relating to the data subject and the data subject exercises his or her right of access without specifying whether it relates to all or part of the data, the controller may request, before providing the information, that the data subject specifies the data or processing activities to which the request relates.

2. The right of access shall be deemed to be granted if the data controller provides the data subject with a remote, direct and secure access system to the personal data that guarantees, on a permanent basis, access to the entirety of the data. For such purposes, the communication by the data controller to the data subject of the manner in which he/she may access such system shall be sufficient to consider the request to exercise the right as granted.

However, the data subject may request from the data controller the information referred to in Article 15(1) of Regulation (EU) 2016/679 that is not included in the remote access system.

3. For the purposes set forth in Article 12.5 of Regulation (EU) 2016/679, the exercise of the right of access on more than one occasion during the six-month period may be considered repetitive, unless there is legitimate cause to do so.

4. Where the data subject chooses a means other than the one offered that entails a disproportionate cost, the request shall be considered excessive, and the data subject shall bear the excess costs that his or her choice entails. In this case, the data controller shall only be required to satisfy the right of access without undue delay.

Article 14. *Right of rectification.*

To exercise the right of rectification recognized in Article 16 of Regulation (EU) 2016/679, the data subject must indicate in his request to which data he refers and the correction to be made. He/she shall accompany, where necessary, the documentation justifying the inaccuracy or incompleteness of the data undergoing processing.

Article 15. *Right of suppression.*

1. The right of deletion shall be exercised in accordance with the provisions of Article 17 of Regulation (EU) 2016/679.

2. Where the erasure results from the exercise of the right to object pursuant to Article 21(2) of Regulation (EU) 2016/679, the controller may retain the data subject's identifying data necessary to prevent future processing for direct marketing purposes.

Article 16. *Right to limitation of processing.*

1. The right to the limitation of processing shall be exercised in accordance with the following provisions in Article 18 of Regulation (EU) 2016/679.

2. The fact that the processing of personal data is limited must be clearly stated in the data controller's information systems.

Article 17. *Right to prunability.*

The right to portability shall be exercised in accordance with the provisions of Article 20 of Regulation (EU) 2016/679.

Article 18. *Right of opposition.*

The right to object, as well as the rights related to automated individual decisions, including profiling, shall be exercised in accordance with the provisions of, respectively, Articles 21 and 22 of Regulation (EU) 2016/679.

TITLE IV

Provisions applicable to specific treatments

Article 19. *Processing of contact, individual entrepreneur and liberal professional data.*

1. In the absence of evidence to the contrary, the processing of contact data and, where appropriate, data relating to the function or position held of natural persons providing services in a legal person shall be presumed to be covered by the provisions of Article 6(1)(f) of Regulation (EU) 2016/679 provided that the following requirements are met:

a) That the processing refers only to the data necessary for their professional location.

b) That the purpose of the processing is solely to maintain relations of any kind with the legal entity in which the data subject provides services.

2. The same presumption shall operate for the processing of data relating to sole proprietors and liberal professionals, when it refers to them only in that capacity and is not processed for the purpose of establishing a relationship with them as natural persons.

3. The data controllers or processors referred to in Article 77.1 of this Organic Law may also process the data referred to in the two preceding paragraphs when this arises from a legal obligation or is necessary for the exercise of their powers.

Article 20. *Credit information systems.*

1. In the absence of evidence to the contrary, the processing of personal data relating to the non-fulfillment of monetary, financial or credit obligations by common credit information systems shall be presumed lawful when the following requirements are met:

a) That the data have been provided by the creditor or by anyone acting on his behalf or in his interest.

b) The data must refer to certain debts, due and payable, the existence or amount of which has not been the subject of an administrative or judicial claim by the debtor or through a binding alternative dispute resolution procedure between the parties.

c) That the creditor has informed the affected party in the contract or at the time of requesting payment of the possibility of inclusion in such systems, indicating those in which it participates.

The entity that maintains the credit information system with data relating to non-compliance with monetary, financial or credit obligations shall notify the affected party of the inclusion of such data and inform him/her of the possibility of exercising the rights set forth in Articles 15 to 22 of Regulation (EU) 2016/679 within thirty days following the notification of the debt to the system, with the data remaining blocked during that period.

d) That the data will only be kept in the system as long as the non-compliance persists, with a maximum limit of five years from the maturity date of the monetary, financial or credit obligation.

e) That data referring to a specific debtor may only be consulted when the person consulting the system maintains a contractual relationship with the affected party that involves the payment of a monetary amount or has requested the conclusion of a contract involving financing, deferred payment or periodic invoicing, as is the case, among other cases, in those provided for in the legislation on consumer credit contracts and real estate credit contracts.

When the right to limit the processing of data has been exercised before the system by contesting its accuracy as provided for in Article 18.1.a) of Regulation (EU) 2016/679, the system will inform those who could consult it pursuant to the preceding paragraph about the mere existence of such circumstance, without providing the specific data in respect of which the right has been exercised, pending the resolution of the data subject's request.

f) In the event that the request to enter into the contract is denied, or the contract is not entered into, as a result of the consultation made, the person who consulted the system shall inform the affected party of the result of such consultation.

2. The entities that maintain the system and the creditors, with respect to the processing of the data referring to their debtors, will have the status of co-responsible for the processing of the data, being applicable the provisions of Article 26 of Regulation (EU) 2016/679.

The creditor shall be responsible for guaranteeing that the requirements for the inclusion of the debt in the system are met, and shall be liable for their non-existence or inaccuracy.

3. The presumption referred to in paragraph 1 of this article does not cover cases in which the credit information was associated by the entity maintaining the system with information additional to that referred to in that paragraph, related to the debtor and obtained from other sources, in order to carry out a profiling of the debtor, in particular through the application of credit rating techniques.

Article 21. *Treatment related to the performance of certain commercial transactions.*

1. Unless there is evidence to the contrary, the processing of data, including their prior communication, which may arise from the development of any operation for the structural modification of companies or the contribution or transfer of a business or branch of business activity, shall be presumed to be lawful, provided that the processing is necessary for the successful completion of the operation and guarantees, where appropriate, the continuity of the provision of services.

2. In the event that the operation is not concluded, the transferee entity shall immediately proceed to the deletion of the data, without the obligation of blocking provided for in this Organic Law being applicable.

Article 22. *Processing for video surveillance purposes.*

1. Natural or legal persons, public or private, may carry out the processing of images through camera or video camera systems for the purpose of preserving the security of persons and property, as well as their facilities.

2. Images of the public road may only be captured insofar as it is essential for the purpose mentioned in the previous paragraph.

However, it will be possible to capture a larger area of the public road when necessary to ensure the security of strategic assets or installations or transport-related infrastructures, but in no case may it involve the capture of images of the interior of a private home.

3. The data will be deleted within a maximum period of one month from its capture, except when they have to be kept to prove the commission of acts that threaten the integrity of persons, property or facilities. In such a case, the images must be made available to the competent authority within a maximum period of seventy-two hours from the time of knowledge of the existence of the recording.

The blocking obligation provided for in Article 32 of this Organic Law shall not apply to such processing.

4. The duty to provide information provided for in Article 12 of Regulation (EU) 2016/679 shall be deemed to be fulfilled by the affixing of an information device in a sufficiently visible place identifying, at least, the existence of the processing, the identity

of the data controller and the possibility of exercising the rights provided for in Articles 15 to 22 of Regulation (EU) 2016/679. A connection code or internet address to this information may also be included in the information device.

In any case, the data controller must keep the information referred to in the aforementioned regulation at the disposal of the data subjects.

5. Under Article 2(2)(c) of Regulation (EU) 2016/679, the processing by a natural person of images that only capture the interior of his or her own home is considered excluded from its scope.

This exclusion does not cover the processing carried out by a private security entity that has been contracted for the surveillance of a home and has access to the images.

6. The processing of personal data from images and sounds obtained through the use of cameras and video cameras by the Security Forces and Bodies and by the competent bodies for surveillance and control in prisons and for the control, regulation, surveillance and discipline of traffic, will be governed by the legislation transposing Directive (EU) 2016/680, when the processing is for the purposes of prevention, investigation, detection or prosecution of criminal offenses or enforcement of criminal penalties, including the protection and prevention against threats to public safety. Outside these cases, such processing shall be governed by its specific legislation and supplemented by Regulation (EU) 2016/679 and this Organic Law.

7. The provisions of this article are without prejudice to the provisions of Law 5/2014, of April 4, 2014, on Private Security and its implementing provisions.

8. The processing by the employer of data obtained through camera or video camera systems is subject to the provisions of Article 89 of this Organic Law.

Article 23. *Advertising exclusion systems.*

1. The processing of personal data with the purpose of preventing the sending of commercial communications to those who have expressed their refusal or opposition to receive them shall be lawful.

For this purpose, general or sectorial information systems may be created, which will only include the data necessary to identify the data subjects. These systems may also include preference services, whereby those affected may limit the receipt of commercial communications to those from certain companies.

2. The entities responsible for the advertising exclusion systems shall inform the competent supervisory authority of their creation, their general or sectorial nature, as well as the way in which those affected may join them and, where appropriate, assert their preferences.

The competent control authority shall make public in its electronic headquarters a list of the systems of this nature that were communicated to it, incorporating the information mentioned in the previous paragraph. To this effect, the competent control authority to which the creation of the system has been communicated shall inform the other control authorities for publication by all of them.

3. When a data subject expresses to a data controller his or her wish not to have his or her data processed for the sending of commercial communications, the data controller shall inform him or her of the existing advertising exclusion systems, and may refer to the information published by the competent supervisory authority.

4. Those who intend to carry out direct marketing communications must first consult the advertising exclusion systems that may affect their actions, excluding from the processing the data of those affected who have expressed their opposition or refusal to it. For these purposes, in order to consider the above obligation fulfilled, it will be sufficient to consult the exclusion systems included in the list published by the competent supervisory authority.

code: BO-EA- 201-8 16673
Verifiable at http //www.boe.es

It shall not be necessary to carry out the consultation referred to in the preceding paragraph when the affected party has given, in accordance with the provisions of this Organic Law, its consent to receive the communication to whoever intends to carry it out.

Article 24. *Internal complaint information systems.*

1. It shall be lawful to create and maintain information systems through which a private law entity may be informed, even anonymously, of the commission within the entity or in the actions of third parties contracting with it, of acts or conduct that may be contrary to the general or sectorial regulations applicable to it. Employees and third parties must be informed of the existence of these information systems.

2. Access to the data contained in these systems shall be limited exclusively to those who, whether or not they are part of the entity, carry out the internal control and compliance functions, or to the persons in charge of the processing that may be appointed for such purpose. However, their access by other persons, or even their communication to third parties, shall be lawful when necessary for the adoption of disciplinary measures or for the processing of legal proceedings, as the case may be.

Without prejudice to the notification to the competent authority of facts constituting a criminal or administrative offense, only when disciplinary measures may be taken against an employee, such access shall be granted to personnel with human resources management and control functions.

3. The necessary measures must be taken to preserve the identity and guarantee the confidentiality of the data corresponding to the persons affected by the information provided, especially that of the person who brought the facts to the entity's attention, in the event that he/she has been identified.

4. The data of the person making the report and of the employees and third parties shall be kept in the reporting system only for the time necessary to decide whether to initiate an investigation into the facts reported.

In any case, three months after the data have been entered, they must be deleted from the reporting system, unless the purpose of the storage is to leave evidence of the functioning of the model for the prevention of the commission of crimes by the legal person. The reports that have not been followed up may only be recorded in anonymized form, without the obligation of blocking provided for in article 32 of this Organic Law being applicable.

Once the period mentioned in the preceding paragraph has elapsed, the data may continue to be processed by the body responsible, in accordance with section 2 of this article, for the investigation of the reported facts, and shall not be kept in the internal complaints information system itself.

5. The principles of the preceding paragraphs shall be applicable to the internal complaint systems that may be created in the Public Administrations.

Article 25. *Data processing in the scope of the public statistical function.*

1. The processing of personal data carried out by the bodies entrusted with the competences related to the exercise of the public statistical function shall be subject t o the provisions of their specific legislation, as well as of Regulation (EU) 2016/679 and of this Organic Law.

2. The communication of data to the competent bodies in statistical matters shall only be understood to be covered by Article 6.1 e) of Regulation (EU) 2016/679 in cases in which the statistics for which the information is required are required by a rule of European Union law or are included in the statistical programming instruments legally provided for.

In accordance with the provisions of Article 11.2 of Law 12/1989, of May 9, 1989, on the Public Statistical Function, they shall be of strictly voluntary contribution and, in

Consequently, only the data referred to in Articles 9 and 10 of Regulation (EU) 2016/679 may be collected with the express consent of the data subjects.

3. The competent bodies for the exercise of the public statistical function may refuse requests for the exercise by data subjects of the rights set forth in Articles 15 to 22 of Regulation (EU) 2016/679 when the data are covered by the guarantees of statistical confidentiality provided for in state or autonomous community legislation.

Article 26. *Processing of data for archiving purposes in the public interest by public administrations.*

The processing by Public Administrations of data for archiving purposes in the public interest shall be lawful and shall be subject to the provisions of Regulation (EU) 2016/679 and of this Organic Law with the specialties deriving from the provisions of Law 16/1985, of 25 June, on Spanish Historical Heritage, in Royal Decree 1708/2011, of November 18, which establishes the Spanish Archive System and regulates the Archive System of the General State Administration and its Public Bodies and its access regime, as well as the applicable autonomous legislation.

Article 27. *Processing of data related to administrative infractions and sanctions.*

1. For the purposes of Article 86 of Regulation (EU) 2016/679, the processing of data relating to administrative offenses and sanctions, including the maintenance of records related thereto, shall require:

a) That the persons in charge of such processing are the competent bodies for the investigation of the sanctioning procedure, for the declaration of infringements or the imposition of sanctions.

b) That the processing is limited to the data strictly necessary for the purpose for which it was carried out.

2. When any of the conditions set forth in the preceding paragraph are not met, the processing of data relating to administrative offenses and penalties must have the consent of the data subject or be authorized by a regulation with the rank of law, which shall regulate, where appropriate, additional guarantees for the rights and freedoms of the data subjects.

3. Apart from the cases indicated in the previous paragraphs, the processing of data referring to administrative infractions and sanctions will only be possible when they are carried out by lawyers and attorneys and their purpose is to collect the information provided by their clients for the exercise of their functions.

TITLE V

Data controller and data processor

CHAPTER I

General provisions. Active liability measures

Article 28. *General obligations of the data controller and data processor.*

1. Controllers and processors shall, taking into account the elements listed in Articles 24 and 25 of Regulation (EU) 2016/679, determine the appropriate technical and organizational measures to be implemented in order to ensure and demonstrate that the processing is in compliance with the said Regulation, with this Organic Law, its implementing rules and the applicable sectoral legislation. In particular, they shall assess whether

the performance of the data protection impact assessment and the prior consultation referred to in Section 3 of Chapter IV of the aforementioned regulation.

2. For the adoption of the measures referred to in the previous paragraph, controllers and processors shall take into account, in particular, the increased risks that could occur in the following cases:

a) When the processing could generate situations of discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data subject to professional secrecy, unauthorized reversal of pseudonymization or any other significant economic, moral or social damage to those affected.

b) When the processing could deprive data subjects of their rights and freedoms or could prevent them from exercising control over their personal data.

c) Where there is processing that is not merely incidental or ancillary to the special categories of data referred to in Articles 9 and 10 of Regulation (EU) 2016/679 and 9 and 10 of this Organic Law or data related to the commission of administrative offenses.

d) When the processing involves an evaluation of personal aspects of the data subjects for the purpose of creating or using personal profiles of the data subjects, in particular by analyzing or predicting aspects relating to their work performance, financial situation, health, personal preferences or interests, reliability or behavior, financial solvency, location or movements.

e) When the processing of data of affected groups in a situation of special vulnerability and, in particular, of minors and people with disabilities is carried out.

f) When there is a massive processing involving a large number of data subjects or involving the collection of a large amount of personal data.

g) When the personal data were to be transferred, on a regular basis, to third States or international organizations for which an adequate level of protection has not been declared.

h) Any others that in the opinion of the person in charge or the person in charge could be relevant and in particular those provided for in codes of conduct and standards defined by certification schemes.

Article 29. *Cases of co-responsibility in the treatment.*

The determination of the responsibilities referred to in Article 26.1 of Regulation (EU) 2016/679 shall be made on the basis of the activities actually carried out by each of the joint controllers.

Article 30. *Representatives of controllers or processors not established in the European Union.*

1. In cases where Regulation (EU) 2016/679 is applicable to a controller or processor not established in the European Union by virtue of the provisions of Article 3.2 thereof and the processing relates to data subjects located in Spain, the Spanish Data Protection Agency or, where appropriate, the regional data protection authorities may impose on the representative, jointly and severally with the controller or processor, the measures set forth in Regulation (EU) 2016/679.

This requirement shall be without prejudice to any liability that may correspond to the data controller or data processor and to the exercise by the representative of the right of recourse against whoever may be liable.

2. Likewise, in the event of a claim for liability under the terms provided for in Article 82 of Regulation (EU) 2016/679, the persons responsible, persons in charge and representatives shall be jointly and severally liable for the damages caused.

Article 31. *Registration of treatment activities.*

1. Controllers and processors or, where applicable, their representatives shall keep the register of processing activities referred to in Article 30 of Regulation (EU) 2016/679, unless the exception provided for in paragraph 5 thereof applies.

The register, which may be organized around structured sets of data, must specify, according to its purposes, the processing activities carried out and the other circumstances established in the aforementioned regulation.

Where the controller or processor has appointed a data protection officer, he/she shall notify him/her of any additions, modifications or deletions to the contents of the register.

2. The subjects listed in Article 77.1 of this Organic Law shall make public an inventory of their processing activities accessible by electronic means containing the information set out in Article 30 of Regulation (EU) 2016/679 and its legal basis.

Article 32. *Blocking of data.*

1. The data controller is obliged to block the data when it is rectified or deleted.

2. The blocking of the data consists of the identification and reservation of the data, adopting technical and organizational measures to prevent its processing, including its visualization, except for making the data available to the judges and courts, the Public Prosecutor's Office or the competent Public Administrations, in particular the data protection authorities, for the demand of possible responsibilities derived from the processing and only for the period of prescription of the same.

Once this period has elapsed, the data must be destroyed.

3. The blocked data may not be processed for any purpose other than that indicated in the previous paragraph.

4. When, in order to comply with this obligation, the configuration of the information system does not allow blocking or requires an adaptation that implies a disproportionate effort, the information shall be securely copied in such a way that digital evidence, or evidence of another nature, shall be recorded to accredit its authenticity, the date of blocking and the non-manipulation of the data during blocking.

5. The Spanish Data Protection Agency and the autonomous data protection authorities, within the scope of their respective competences, may establish exceptions to the obligation to block established in this article, in those cases in which, given the nature of the data or the fact that they refer to a particularly large number of data subjects, their mere conservation, even blocked, could generate a high risk for the rights of the data subjects, as well as in those cases in which the conservation of the blocked data could imply a disproportionate cost for the data controller.

CHAPTER II

Data Processor

Article 33. *Data processor.*

1. Access by a processor to personal data that are necessary for the provision of a service to the controller shall not be considered communication of data provided that the provisions of Regulation (EU) 2016/679, this Organic Law and its implementing rules are complied with.

2. A person shall be considered a data controller and not a processor if, in his or her own name and without being acting on behalf of another person, he or she establishes

relations with data subjects even if there is a contract or legal act with the content set out in Article 28(3) of Regulation (EU) 2016/679. This provision shall not apply to processing orders carried out within the framework of public sector procurement legislation.

The data controller shall also be considered as the person in charge of the processing who uses the data for his own purposes.

3. The controller shall determine whether, upon termination of the services of the processor, the personal data should be destroyed, returned to the controller or given to a new processor, as the case may be.

The destruction of the data will not proceed when there is a legal provision that obliges their conservation, in which case they must be returned to the person in charge, who will guarantee their conservation as long as such obligation persists.

4. The data processor may keep the data, duly blocked, for as long as liabilities may arise from its relationship with the data controller.

5. Within the scope of the public sector, the powers of a data processor may be attributed to a specific body of the General State Administration, the Administration of the Autonomous Communities, the Entities that make up the Local Administration or to the Bodies linked to or dependent on them through the adoption of a rule regulating such powers, which must incorporate the content required by Article 28.3 of Regulation (EU) 2016/679.

CHAPTER III

Data Protection Officer

Appointment of a data protection officer.

1. Controllers and processors shall appoint a data protection officer in the cases provided for in Article 37.1 of Regulation (EU) 2016/679 and, in any case, in the case of the following entities:

a) Professional associations and their general councils.

b) Schools offering education at any of the levels established in the legislation regulating the right to education, as well as public and private universities.

c) Entities operating electronic communications networks and providing electronic communications services in accordance with the provisions of their specific legislation, when they routinely and systematically process personal data on a large scale.

d) Providers of information society services when they elaborate large-scale profiles of service users.

e) The entities included in Article 1 of Law 10/2014, of June 26, on the regulation, supervision and solvency of credit institutions.

f) Financial credit institutions.

g) Insurance and reinsurance companies.

h) Investment services companies, regulated by the Securities Market legislation.

i) Electric power distributors and marketers and natural gas distributors and marketers.

j) The entities responsible for common files for the evaluation of solvency and creditworthiness or common files for the management and prevention of fraud, including those responsible for the files regulated by the legislation for the prevention of money laundering and the financing of terrorism.

k) Entities that carry out advertising and commercial prospecting activities, including commercial and market research activities, when they conduct

processing based on the preferences of the data subjects or perform activities involving profiling of the data subjects.

l) Health centers legally obliged to keep patients' medical records.

Exceptions are health professionals who, although legally obliged to keep patients' medical records, carry out their activity on an individual basis.

m) The entities that have as one of their objects the issuance of commercial reports that may refer to natural persons.

n) Operators that develop the gaming activity through electronic, computerized, telematic and interactive channels, in accordance with the gaming regulation regulations.

ñ) Private security companies.

o) Sports federations when processing data of minors.

2. Data controllers or processors not included in the preceding paragraph may voluntarily appoint a data protection officer, who shall be subject to the regime established in Regulation (EU) 2016/679 and in this Organic Law.

3. Data controllers and data processors shall communicate within ten days to the Spanish Data Protection Agency or, as the case may be, to the regional data protection authorities, the designations, appointments and dismissals of the data protection officers both in the cases in which they are obliged to designate them and in the case in which their designation is voluntary.

4. The Spanish Data Protection Agency and the regional data protection authorities will maintain, within the scope of their respective competences, an updated list of data protection officers, which will be accessible by electronic means.

5. In fulfilling the obligations of this article, controllers and processors may establish the full or part-time dedication of the delegate, among other criteria, depending on the volume of processing, the special category of data processed or the risks to the rights or freedoms of data subjects.

Article 35. *Qualification of the data protection officer.*

Compliance with the requirements set forth in Article 37.5 of Regulation (EU) 2016/679 for the appointment of the data protection officer, whether a natural or legal person, may be demonstrated, among other means, through voluntary certification mechanisms that shall take particular account of obtaining a university degree attesting to specialized knowledge in data protection law and practice.

Position of the data protection officer.

1. The data protection officer will act as the interlocutor of the data controller or data processor before the Spanish Data Protection Agency and the regional data protection authorities. The delegate may inspect the procedures related to the object of this Organic Law and issue recommendations within the scope of his or her competences.

2. In the case of a natural person within the organization of the data controller or data processor, the data protection officer may not be removed or penalized by the controller or data processor for performing his or her duties, unless he or she is guilty of wilful misconduct or gross negligence in the performance of his or her duties. The independence of the data protection officer within the organization shall be guaranteed, and any conflict of interest shall be avoided.

3. In the exercise of his functions, the data protection officer shall have access to personal data and processing processes, and the data controller or data processor may not oppose this access to the existence of any duty of confidentiality or secrecy, including that provided for in Article 5 of this Organic Law.

4. When the data protection officer becomes aware of a relevant breach of data protection, he/she shall document it and immediately inform the administrative and management bodies of the controller or processor.

Intervention of the data protection officer in the event of a complaint to the data protection authorities.

1. When the data controller or processor has appointed a data protection officer, the data subject may, prior to filing a complaint against them before the Spanish Data Protection Agency or, where appropriate, before the regional data protection authorities, contact the data protection officer of the entity against which the complaint is made.

In this case, the data protection officer shall inform the data subject of the decision taken within a maximum period of two months from receipt of the complaint.

2. When the data subject files a complaint with the Spanish Data Protection Agency or, as the case may be, with the regional data protection authorities, the latter may forward the complaint to the data protection officer so that he/she may respond within one month.

If after this period the data protection officer has not informed the competent data protection authority of the response to the complaint, said authority shall continue the procedure in accordance with the provisions of Title VIII of this Organic Law and its implementing rules.

3. The procedure before the Spanish Data Protection Agency will be that established in Title VIII of this Organic Law and in its implementing regulations. Likewise, the autonomous communities shall regulate the corresponding procedure before their autonomous data protection authorities.

CHAPTER IV

Codes of conduct and certification

Article 38. *Codes of Conduct.*

1. The codes of conduct regulated by Section 5.ª of Chapter IV of Regulation (EU) 2016/679 shall be binding on those who adhere to them.

These codes may include mechanisms for the extrajudicial resolution of conflicts.

2. Such codes may be promoted, in addition to the associations and bodies referred to in Article 40.2 of Regulation (EU) 2016/679, by companies or groups of companies as well as by the managers or persons in charge referred to in Article 77.1 of this Organic Law.

They may also be promoted by the bodies or entities that assume the functions of supervision and out-of-court dispute resolution referred to in Article 41 of Regulation (EU) 2016/679.

Data controllers or processors who adhere to the code of conduct are obliged to submit to the supervisory body or entity any complaints made to them by data subjects in relation to the processing of data included in its scope of application in the event that they consider that it is not appropriate to meet the request in the complaint, without prejudice to the provisions of article 37 of this Organic Law. In addition, without prejudice to the powers conferred by Regulation (EU) 2016/679 on the

data protection authorities, may, on a voluntary basis and prior to carrying out the processing, submit to the said supervisory body or entity the verification of the compliance of the processing with the matters subject to the code of conduct.

In the event that the supervisory body or entity rejects or dismisses the complaint, or if the controller or processor does not submit the complaint to its decision, the data subject may file a complaint with the Spanish Data Protection Agency or, where appropriate, the regional data protection authorities.

The competent data protection authority shall verify that the bodies or entities promoting the codes of conduct have provided these codes with supervisory bodies that meet the requirements set out in Article 41(2) of Regulation (EU) 2016/679.

3. The codes of conduct shall be approved by the Spanish Data Protection Agency or, as the case may be, by the competent regional data protection authority.

4. The Spanish Data Protection Agency or, where appropriate, the regional data protection authorities shall submit the draft codes to the consistency mechanism referred to in Article 63 of Regulation (EU) 2016/679 in the cases in which this is appropriate according to its Article 40.7. The procedure shall be suspended as long as the European Data Protection Committee does not issue the opinion referred to in Articles 64.1.b) and 65.1.c) of the aforementioned regulation.

When it is an autonomous data protection authority that submits the draft code to the consistency mechanism, the provisions of article 60 of this Organic Law shall apply.

5. The Spanish Data Protection Agency and the autonomous data protection authorities shall keep registers of the codes of conduct approved by them, which shall be interconnected with each other and coordinated with the register managed by the European Data Protection Committee in accordance with article 40.11 of the aforementioned regulation.

The registry will be accessible through electronic means.

6. A Royal Decree will establish the content of the registry and the special features of the procedure for the approval of the codes of conduct.

Article 39. *Accreditation of ceding institutions.*

Without prejudice to the functions and powers of accreditation of the competent supervisory authority under Articles 57 and 58 of Regulation (EU) 2016/679, the accreditation of the certification bodies referred to in Article 43.1 of said Regulation may be carried out by the National Accreditation Body (ENAC), which shall inform the Spanish Data Protection Agency and the data protection authorities of the autonomous communities of the grants, refusals or revocations of accreditations, as well as the reasons for such grants, refusals or revocations.

TITLE VI

International data transfers

Article 40. *Regime for international data transfers.*

International data transfers shall be governed by the provisions of Regulation (EU) 2016/679, this Organic Law and its implementing regulations approved by the Government, and the circulars of the Spanish Data Protection Agency and the autonomous data protection authorities, within the scope of their respective competences.

In any case, the provisions contained in these rules, in particular those governing the principles of data protection, shall apply to the processing operations involved in the transfer itself.

Article 41. *Cases of adoption by the Spanish Data Protection Agency.*

1. The Spanish Data Protection Agency and the autonomous data protection authorities may adopt, in accordance with the provisions of Article 46.2.c) of Regulation (EU) 2016/679, standard contractual clauses for the performance of international data transfers, which shall be previously submitted to the opinion of the European Data Protection Committee provided for in Article 64 of the aforementioned regulation.

2. The Spanish Data Protection Agency and the regional data protection authorities may approve binding corporate rules in accordance with the provisions of Article 47 of Regulation (EU) 2016/679.

The procedure shall be initiated at the request of an entity located in Spain and shall have a maximum duration of nine months. It will be suspended as a result of the referral of the file to the European Data Protection Committee for it to issue the opinion referred to in Article 64.1.f) of Regulation (EU) 2016/679, and will continue after its notification to the Spanish Data Protection Agency or to the competent autonomous data protection authority.

Article 42. *Cases subject to prior authorization by the data protection authorities.*

1. International transfers of data to countries or international organizations that do not have an adequacy decision approved by the Commission or that are not covered by any of the guarantees provided for in the previous article and in Article 46.2 of Regulation (EU) 2016/679, shall require prior authorization from the Spanish Data Protection Agency or, where appropriate, autonomous data protection authorities, which may be granted in the following cases:

a) Where the transfer purports to be based on the provision of adequate guarantees on the basis of contractual clauses that do not correspond to the standard clauses provided for in Article 46(2)(c) and (d) of Regulation (EU) 2016/679.

b) When the transfer is carried out by any of the persons responsible or in charge referred to in Article 77.1 of this Organic Law and is based on provisions incorporated in non-regulatory international agreements with other authorities or public bodies of third States, which incorporate effective and enforceable rights for those affected, including memorandums of understanding.

The procedure will have a maximum duration of six months.

2. The authorization shall be subject to the issuance by the European Data Protection Committee of the opinion referred to in Articles 64.1.e), 64.1.f) and 65.1.c) of Regulation (EU) 2016/679. The referral of the file to the aforementioned committee shall imply the suspension of the procedure until the opinion is notified to the Spanish Data Protection Agency or, through the same, to the competent supervisory authority, as the case may be.

Article 43. *Cases subject to prior information to the competent data protection authority.*

Data controllers shall inform the Spanish Data Protection Agency or, where appropriate, the regional data protection authorities, of any international transfer of data that they intend to carry out on the basis of its necessity for purposes related to compelling legitimate interests pursued by them and the concurrence of the rest of the requirements provided for in the last paragraph of Article 49.1 of Regulation (EU) 2016/679. They shall also inform the data subjects of the transfer and of the overriding legitimate interests pursued.

This information must be provided prior to the transfer.

The provisions of this Article shall not apply to activities carried out by public authorities in the exercise of their public powers in accordance with Article 49(3) of Regulation (EU) 2016/679.

TITLE VII

Data Protection Authorities

CHAPTER I

The Spanish Data Protection Agency

Section 1. General Provisions.

Article 44. *General Provisions.*

1. The Spanish Data Protection Agency is an independent administrative authority of state scope, of those provided for in Law 40/2015, of October 1, on the Legal Regime of the Public Sector, with legal personality and full public and private capacity, which acts with full independence from the public authorities in the exercise of its functions.

Its official name, in accordance with the provisions of Article 109.3 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector, shall be "Spanish Data Protection Agency, Independent Administrative Authority".

It relates to the Government through the Ministry of Justice.

2. The Spanish Data Protection Agency shall be the common representative of the data protection authorities of the Kingdom of Spain in the European Data Protection Committee.

3. The Spanish Data Protection Agency and the General Council of the Judiciary shall collaborate for the proper exercise of the respective competences that the Organic Law 6/1985, of July 1, 1985, of the Judiciary, attributes to them in matters of personal data protection within the scope of the Administration of Justice.

Article 45. *Legal Regime.*

1. The Spanish Data Protection Agency is governed by the provisions of Regulation (EU) 2016/679, this Organic Law and its implementing provisions.

In addition, insofar as it is compatible with its full independence and without prejudice to the provisions of Article 63.2 of this Organic Law, it shall be governed by the rules referred to in Article 110.1 of Law 40/2015, of October 1, on the Legal Regime of the Public Sector.

2. The Government, at the proposal of the Spanish Data Protection Agency, will approve its Statute by Royal Decree.

Article 46. *Economic, budgetary and personnel regime.*

1. The Spanish Data Protection Agency will prepare and approve its budget and will send it to the Government so that it may be integrated, independently, in the General State Budget.

2. The system of modifications and linkage of the appropriations of its budget shall be that established in the Statute of the Spanish Data Protection Agency.

The Presidency of the Spanish Data Protection Agency is responsible for authorizing budgetary modifications involving up to three percent of the initial figure of its total expenditure budget, provided that the appropriations for personnel expenses are not increased. The remaining modifications that do not exceed five per cent of the initial figure of the

The budget shall be authorized by the Ministry of Finance and, in other cases, by the Government.

3. The Spanish Data Protection Agency will count for the fulfillment of its purposes with the allocations that are established from the General State Budget, the assets and securities that constitute its patrimony and the income, ordinary and extraordinary derived from the exercise of its activities, including those derived from the exercise of the powers established in Article 58 of Regulation (EU) 2016/679.

4. The positive result of its income will be allocated by the Spanish Data Protection Agency to the endowment of its reserves in order to guarantee its full independence.

5. The personnel at the service of the Spanish Data Protection Agency shall be civil servants or employees and shall be governed by the provisions of the revised text of the Law of the Basic Statute of the Public Employee, approved by Royal Legislative Decree 5/2015, of October 30, and other regulations governing civil servants and, where appropriate, by labor regulations.

6. The Spanish Data Protection Agency shall draw up and approve its list of posts, within the framework of the criteria established by the Ministry of Finance, respecting the limit of personnel expenditure established in the budget. This list of posts will include, in any case, those posts that must be held exclusively by civil servants, as they consist of the exercise of functions that imply direct or indirect participation in the exercise of public powers and the safeguarding of the general interests of the State and of the Public Administrations.

7. Without prejudice to the powers attributed to the Court of Auditors, the economic-financial management of the Spanish Data Protection Agency shall be subject to the control of the General Comptroller of the State Administration under the terms established in Law 47/2003, of 26 November, General Budgetary Law.

Article 47. *Functions and powers of the Spanish Data Protection Agency.*

The Spanish Data Protection Agency is responsible for supervising the application of this Organic Law and Regulation (EU) 2016/679 and, in particular, for exercising the functions established in Article 57 and the powers provided for in Article 58 of the same regulation, in this Organic Law and in its implementing provisions.

Likewise, the Spanish Data Protection Agency is responsible for the performance of the functions and powers attributed to it by other laws or regulations of European Union Law.

The Presidency of the Spanish Data Protection Agency.

1. The Presidency of the Spanish Data Protection Agency directs it, represents it and issues its resolutions, circulars and guidelines.

2. The Presidency of the Spanish Data Protection Agency shall be assisted by a Deputy to whom it may delegate its functions, with the exception of those related to the procedures regulated by Title VIII of this Organic Law, and who shall substitute it in the exercise of the same under the terms provided in the Organic Statute of the Spanish Data Protection Agency.

Both shall exercise their functions with full independence and objectivity and shall not be subject to any instruction in their performance. The legislation regulating the exercise of senior positions in the General State Administration shall be applicable to them.

3. The Presidency of the Spanish Data Protection Agency and its Deputy shall be appointed by the Government, at the proposal of the Ministry of Justice, from among persons of recognized professional competence, particularly in the field of data protection.

Two months prior to the expiration of the term of office or, in the case of other causes for dismissal, when the latter has occurred, the Ministry of Justice shall order the publication in the Official State Gazette of the public call for candidates.

After evaluating the merit, capacity, competence and suitability of the candidates, the Government shall submit to the Congress of Deputies a proposal for the Presidency and Deputy, accompanied by a report justifying it, which, after holding the mandatory hearing of the candidates, shall be ratified by the Justice Committee in a public vote by a majority of three-fifths of its members in the first vote or, if this is not reached, by an absolute majority in the second vote, which shall be held immediately after the first vote. In the latter case, the votes in favor must come from Members belonging to at least two different parliamentary groups.

4. The Presidency and the Deputy of the Spanish Data Protection Agency will be appointed by the Council of Ministers by Royal Decree.

5. The term of office of the Presidency and the Deputy of the Spanish Data Protection Agency is five years and may be renewed for another term of the same duration.

The Presidency and the Deputy shall only cease before the expiration of their term of office, at their own request or by separation agreed by the Council of Ministers, by:

a) Serious non-compliance with its obligations,
b) supervening incapacity to perform his or her duties,
c) incompatibility, or
d) conviction for an intentional crime.

In the cases provided for in letters a), b) and c), the ratification of the separation by the parliamentary majorities provided for in paragraph 3 of this article shall be necessary.

6. The acts and provisions issued by the Presidency of the Spanish Data Protection Agency put an end to administrative proceedings, and may be appealed directly before the Contentious-Administrative Chamber of the National High Court.

Article 49. *Advisory Council of the Spanish Data Protection Agency.*

1. The Presidency of the Spanish Data Protection Agency will be advised by an Advisory Council composed of the following members:

a) One Deputy, proposed by the Congress of Deputies.
b) One Senator, nominated by the Senate.
c) A representative appointed by the General Council of the Judiciary.
d) A representative of the General State Administration with experience in the field, proposed by the Minister of Justice.
e) A representative of each Autonomous Community that has created a Data Protection Authority in its territorial area, proposed in accordance with the provisions of the respective Autonomous Community.
f) An expert proposed by the Spanish Federation of Municipalities and Provinces.
g) An expert proposed by the Consumers and Users Council.
h) Two experts proposed by the Business Organizations.
i) A representative of data protection and privacy professionals, proposed by the statewide association with the largest number of members.
j) A representative of the bodies or entities for the supervision and extrajudicial resolution of conflicts provided for in Chapter IV of Title V, proposed by the Minister of Justice.
k) An expert, proposed by the Conference of Rectors of Spanish Universities.
l) A representative of the organizations that bring together the General Councils, Higher Councils and Professional Associations at the state level of the different collegiate professions, proposed by the Minister of Justice.
m) A representative of the information security professionals, proposed by the statewide association with the largest number of members.

n) An expert in transparency and access to public information proposed by the Council for Transparency and Good Governance.

ñ) Two experts proposed by the most representative trade union organizations.

2. For the purposes of the preceding paragraph, the status of expert shall require accreditation of specialized knowledge in data protection law and practice through professional or academic practice.

3. The members of the Advisory Council shall be appointed by order of the Minister of Justice, published in the Official State Gazette.

4. The Advisory Council shall meet when so ordered by the Presidency of the Spanish Data Protection Agency and, in any case, once every six months.

5. The decisions taken by the Advisory Council shall in no case be binding.

6. In all matters not provided for in this Organic Law, the regime, competences and operation of the Advisory Council shall be those established in the Organic Statute of the Spanish Data Protection Agency.

Article 50. *Publicity.*

The Spanish Data Protection Agency will publish the resolutions of its Presidency that declare whether or not the rights recognized in Articles 15 to 22 of Regulation (EU) 2016/679 have been granted, those that put an end to the complaint procedures, those that archive the preliminary investigation proceedings, those that sanction the entities referred to in Article 77.1 of this Organic Law with a warning, those that impose precautionary measures and any others provided for in its Statute.

Section 2. "Investigation powers and preventive audit plans

Article 51. *Scope and competent personnel.*

1. The Spanish Data Protection Agency will develop its investigation activity through the actions provided for in Title VIII and the preventive audit plans.

2. The investigation activity will be carried out by officials of the Spanish Data Protection Agency or by officials from outside the Agency expressly authorized by its Presidency.

3. In cases of joint investigative actions in accordance with the provisions of Article 62 of Regulation (EU) 2016/679, the staff of the supervisory authorities of other Member States of the European Union who collaborate with the Spanish Data Protection Agency shall exercise their powers in accordance with the provisions of this Organic Law and under the guidance and in the presence of the staff of the Spanish Data Protection Agency.

4. Officials carrying out investigative activities shall be considered agents of the authority in the performance of their duties, and shall be bound to keep secret any information they may learn in the course of their duties, even after they have ceased to perform them.

Article 52. *Duty of collaboration.*

1. The Public Administrations, including the tax and Social Security Administrations, and individuals shall be obliged to provide the Spanish Data Protection Agency with the data, reports, background information and supporting documents necessary to carry out its investigation activities.

Where the information contains personal data the communication of such data shall be covered by the provisions of Article 6(1)(c) of Regulation (EU) 2016/679.

2. Within the framework of preliminary investigation actions, when the Spanish Data Protection Agency has not been able to carry out the identification by other means, it may request the following from the Public Administrations, including tax and Social Security authorities

Social, information and data that are essential for the sole purpose of identifying those responsible for conduct that could constitute an infringement of Regulation (EU) 2016/679 and this Organic Law.

In the case of the Tax and Social Security Administrations, the information will be limited to that which is necessary to be able to unequivocally identify against whom the Spanish Data Protection Agency must take action in cases of creation of corporate networks that would make it difficult to obtain direct knowledge of the alleged perpetrator of the conduct contrary to Regulation (EU) 2016/679 and to this Organic Law.

3. When it has not been able to carry out the identification by other means, the Spanish Data Protection Agency may request from the operators that provide publicly available electronic communications services and from the providers of information society services the data in its possession that are essential for the identification of the alleged perpetrator of the conduct contrary to Regulation (EU) 2016/679 and to this Organic Law when it has been carried out through the use of an information society service or the making of an electronic communication. For such purposes, the data that the Spanish Data Protection Agency may collect under this section are the following:

a) When the conduct has been carried out through the use of a fixed or mobile telephone service:

1. ° The telephone number of origin of the call in case it has been hidden.
2. ° The name, identification document number and address of the subscriber or registered user to whom the telephone number corresponds.
3. ° The mere confirmation that a specific call has been made between two numbers at a specific date and time.

b) When the conduct has been carried out through the use of an information society service:

1. The identification of the Internet protocol address from which the conduct was carried out and the date and time of the conduct.
2. ° If the conduct was carried out by e-mail, the identification of the Internet protocol address from which the e-mail account was created and the date and time at which it was created.
3. ° The name, identification document number and address of the subscriber or registered user to whom the Internet Protocol address referred to in the two preceding paragraphs has been assigned.

These data must be transferred, upon a reasoned request from the Spanish Data Protection Agency, exclusively within the framework of investigation actions initiated as a result of a complaint filed by an affected party regarding a conduct of a legal person or regarding the use of systems that allow the unrestricted disclosure of personal data. In all other cases, the transfer of this data will require prior judicial authorization granted in accordance with the procedural rules when required.

Excluded from the provisions of this section are traffic data that operators are processing for the sole purpose of complying with the obligations set forth in Law 25/2007, of October 18, 2007, on the conservation of data relating to electronic communications and public communications networks, the transfer of which may only take place in accordance with the provisions thereof, upon prior judicial authorization requested by any of the authorized agents referred to in Article 6 of said Law.

code: BO-EA- 201-8 16673
Verifiable at http ://www.boe.es

Article 53. *Scope of the research activity.*

1. Those carrying out the investigation activity may collect the information necessary for the fulfillment of their functions, carry out inspections, require the exhibition or sending of the necessary documents and data, examine them at the place where they are stored or where the processing is carried out, obtain copies of them, inspect the physical and logical equipment and require the execution of processing and management programs or procedures and support of the processing subject to investigation.

2. When it is necessary for the personnel carrying out the investigative activity to access the constitutionally protected domicile of the inspected person, it will be necessary to have his or her consent or to have obtained the corresponding judicial authorization.

3. In the case of judicial bodies or judicial offices, the exercise of the powers of inspection shall be carried out through and by means of the General Council of the Judiciary.

Article 54. *Audit plans.*

1. The Presidency of the Spanish Data Protection Agency may agree to carry out preventive audit plans, referring to the processing of a specific sector of activity. They will be aimed at analyzing compliance with the provisions of Regulation (EU) 2016/679 and of this Organic Law, based on the performance of research activities on entities belonging to the inspected sector or on the controllers subject to the audit.

2. As a result of the audit plans, the Presidency of the Spanish Data Protection Agency may issue the general or specific guidelines for a specific controller or processor required to ensure the full adaptation of the sector or controller to Regulation (EU) 2016/679 and to this Organic Law.

In the preparation of such guidelines, the Presidency of the Spanish Data Protection Agency may request the collaboration of the supervisory bodies of the codes of conduct and extrajudicial resolution of conflicts, if any.

3. The guidelines shall be mandatory for the sector or manager to which the audit plan refers.

Section 3.ª Other Powers of the Spanish Data Protection Agency

Article 55. *Regulatory powers. Circulars of the Spanish Data Protection Agency.*

1. The Presidency of the Spanish Data Protection Agency may issue provisions establishing the criteria to be followed by this authority in the application of the provisions of Regulation (EU) 2016/679 and this Organic Law, which shall be called "Circulars of the Spanish Data Protection Agency".

2. Its preparation shall be subject to the procedure established in the Statute of the Spanish Data Protection Agency, which shall provide for the necessary technical and legal reports and the hearing of the interested parties.

3. The circulars will be binding once published in the Official State Gazette.

Article 56. *External action.*

1. The Spanish Data Protection Agency is responsible for the ownership and exercise of the functions related to the external action of the State in matters of data protection.

Likewise, the autonomous communities, through the autonomous data protection authorities, are responsible for exercising the functions as subjects of external action within the framework of their powers in accordance with the provisions of Law 2/2014, of 25.

of March, of the Action and Foreign Service of the State, as well as to conclude international administrative agreements in execution and concretization of an international treaty and non-normative agreements with the analogous bodies of other subjects of international law, not legally binding for those who sign them, on matters within its competence within the framework of Law 25/2014, of November 27, of Treaties and other International Agreements.

2. The Spanish Data Protection Agency is the competent body for the protection of natural persons with regard to the processing of personal data arising from the application of any International Convention to which the Kingdom of Spain is a party that attributes to a national supervisory authority such competence and the common representative of the Data Protection authorities in the European Data Protection Committee, in accordance with the provisions of Article 68.4 of Regulation (EU) 2016/679.

The Spanish Data Protection Agency will inform the autonomous data protection authorities of the decisions adopted in the European Data Protection Committee and will seek their opinion on matters within their competence.

3. Without prejudice to the provisions of paragraph 1, the Spanish Data Protection Agency:

a) Participate in international meetings and forums outside the European Union established by mutual agreement of the independent supervisory authorities in the field of data protection.

b) It shall participate, as the Spanish authority, in the international organizations competent in the field of data protection, in the committees or working, study and collaboration groups of international organizations dealing with matters affecting the fundamental right to the protection of personal data and in other international forums or working groups, within the framework of the State's foreign action.

c) It shall collaborate with authorities, institutions, organizations and administrations of other States in order to foster, promote and develop the fundamental right to data protection, particularly in the Ibero-American sphere, and may sign international administrative and non-regulatory agreements on the subject.

CHAPTER II

Autonomous data protection authorities

Section 1.ª General provisions

Article 57. *Autonomous data protection authorities.*

1. The autonomous authorities for the protection of personal data may exercise, the functions and powers established in Articles 57 and 58 of Regulation (EU) 2016/679, in accordance with the autonomous regulations, when they relate to:

a) Treatment for which the entities forming part of the public sector of the corresponding Autonomous Community or of the Local Entities included in its territorial scope or those who provide services through any form of direct or indirect management are responsible.

b) Treatments carried out by individuals or legal entities for the exercise of public functions in matters within the competence of the corresponding Autonomous or Local Administration.

c) Treatments that are expressly provided for, where appropriate, in the respective Statutes of Autonomy.

2. The autonomous data protection authorities may issue, in relation to the processing operations under their jurisdiction, circulars with the scope and effects of the processing operations.

established for the Spanish Data Protection Agency in Article 55 of this Organic Law.

Article 58. *Institutional cooperation.*

The Presidency of the Spanish Data Protection Agency will convene, on its own initiative or when requested by another authority, the autonomous data protection authorities to contribute to the consistent application of Regulation (EU) 2016/679 and this Organic Law. In any case, bi-annual cooperation meetings shall be held.

The Presidency of the Spanish Data Protection Agency and the regional data protection authorities may request and must mutually exchange the information necessary for the fulfillment of their functions and, in particular, that relating to the activity of the European Data Protection Committee. Likewise, they may set up working groups to deal with specific matters of common interest.

Article 59. *Processing contrary to Regulation (EU) 2016/679.*

When the Presidency of the Spanish Data Protection Agency considers that a processing carried out in matters under the competence of the regional data protection authorities violates Regulation (EU) 2016/679, it may require them to adopt, within a period of one month, the necessary measures for its cessation.

If the autonomous authority does not comply with the requirement within the deadline or the measures adopted do not entail the cessation of the unlawful processing, the Spanish Data Protection Agency may bring the appropriate actions before the contentious-administrative jurisdiction.

Section 2." Coordinationunder the procedures set out in Regulation (EU) 2016/679.

Article 60. *Coordination in the event of an opinion being issued by the European Data Protection Committee.*

All communications between the European Data Protection Committee and the autonomous data protection authorities shall be made through the Spanish Data Protection Agency when the latter, as competent authorities, must submit their draft decision to the aforementioned committee or request it to examine a matter pursuant to the provisions of Article 64(1) and (2) of Regulation (EU) 2016/679.

In these cases, the Spanish Data Protection Agency will be assisted by a representative of the Autonomous Authority in its intervention before the Committee.

Article 61. *Intervention in case of cross-border processing.*

1. The autonomous data protection authorities shall have the status of lead supervisory authority or interested party in the procedure established by Article 60 of Regulation (EU) 2016/679 when it refers to a processing operation provided for in Article 57 of this Organic Law that is carried out by a controller or processor provided for in Article 56 of Regulation (EU) 2016/679, unless it significantly develops processing operations of the same nature in the rest of the Spanish territory.

2. In these cases, it will correspond to the autonomous authorities to intervene in the procedures established in Article 60 of Regulation (EU) 2016/679, informing the Spanish Data Protection Agency about its development in the cases in which the consistency mechanism must be applied.

code: BO-EA- 201-8 16673
Verifiable at http ://www.boe.es

Article 62. *Coordination in the event of dispute resolution by the European Data Protection Committee.*

1. All communications between the European Data Protection Board and the autonomous data protection authorities shall be made through the Spanish Data Protection Agency when the latter, as lead authorities, must request the said Board to issue a binding decision as provided for in Article 65 of Regulation (EU) 2016/679.

2. The autonomous data protection authorities that have the status of non-lead interested authority in a procedure of those provided for in Article 65 of Regulation (EU) 2016/679 shall inform the Spanish Data Protection Agency when the matter is referred to the European Data Protection Board, providing it with the documentation and information necessary for its processing.

The Spanish Data Protection Agency will be assisted by a representative of the autonomous authority concerned in its intervention before the aforementioned committee.

TITLE VIII

Procedures in the event of a possible violation of the regulations for the protection of personal data.
data

Article 63. *Legal Regime.*

1. The provisions of this Title shall apply to the procedures processed by the Spanish Data Protection Agency in cases in which a data subject claims that his or her request to exercise the rights recognized in Articles 15 to 22 of Regulation (EU) 2016/679 has not been met, as well as in cases in which the Agency investigates the existence of a possible infringement of the provisions of the aforementioned regulation and of this Organic Law.

2. The procedures processed by the Spanish Data Protection Agency shall be governed by the provisions of Regulation (EU) 2016/679, in this Organic Law, by the regulatory provisions issued in its development and, insofar as they do not contradict them, subsidiarily, by the general rules on administrative procedures.

3. The Government shall regulate by Royal Decree the procedures processed by the Spanish Data Protection Agency under this Title, ensuring in all cases the rights of defense and hearing of the interested parties.

Article 64. *Form of initiation of the procedure and duration.*

1. When the procedure refers exclusively to the lack of attention to a request for the exercise of the rights set forth in Articles 15 to 22 of Regulation (EU) 2016/679, it shall be initiated by an agreement to admit for processing, which shall be adopted in accordance with the provisions of Article 65 of this Organic Law.

In this case, the term to resolve the procedure shall be six months from the date on which the claimant was notified of the decision to admit the claim for processing. Once this period has elapsed, the interested party may consider the claim to have been upheld.

2. When the purpose of the procedure is to determine the possible existence of an infringement of the provisions of Regulation (EU) 2016/679 and of this Organic Law, it shall be initiated by an agreement to initiate the procedure adopted on its own initiative or as a result of a complaint.

If the procedure is based on a complaint filed with the Spanish Data Protection Agency, the latter shall decide on its admission for processing, in accordance with the provisions of Article 65 of this Organic Law.

Where the rules set out in Article 60 of Regulation (EU) 2016/679 apply, the procedure shall be initiated by the adoption of the draft agreement

of the initiation of the sanctioning procedure, of which the interested party shall be formally notified for the purposes set forth in Article 75 of this Organic Law.

Once the complaint has been admitted for processing, as well as in those cases in which the Spanish Data Protection Agency acts on its own initiative, prior to the initiation agreement, there may be a phase of preliminary investigation proceedings, which shall be governed by the provisions of Article 67 of this Organic Law.

The procedure will have a maximum duration of nine months from the date of the initiation agreement or, as the case may be, of the draft initiation agreement. Once this period has elapsed, the procedure will expire and, consequently, the proceedings will be filed.

3. The procedure may also be processed as a result of the communication to the Spanish Data Protection Agency by the supervisory authority of another Member State of the European Union of the complaint made before the same, when the Spanish Data Protection Agency had the status of lead supervisory authority for the processing of a procedure in accordance with the provisions of Articles 56 and 60 of Regulation (EU) 2016/679. The provisions of paragraph 1 and the first, third, fourth and fifth subparagraphs of paragraph 2 shall apply in this case.

4. The processing periods established in this article as well as those for admission for processing regulated by article 65.5 and the duration of the preliminary investigation proceedings provided for in article 67.2, shall be automatically suspended when information, consultation, request for assistance or mandatory pronouncement of a body or agency of the European Union or of one or more supervisory authorities of the Member States must be sought in accordance with the provisions of Regulation (EU) 2016/679, for the time between the request and the notification of the pronouncement to the Spanish Data Protection Agency.

Article 65. *Admission of claims.*

1. When a complaint is submitted to the Spanish Data Protection Agency, the latter shall evaluate its admissibility for processing, in accordance with the provisions of this article.

2. The Spanish Data Protection Agency will not admit the complaints submitted when they do not deal with personal data protection issues, are manifestly unfounded, are abusive or do not provide rational indications of the existence of an infringement.

3. Likewise, the Spanish Data Protection Agency may reject the claim when the data controller or data processor, following a warning issued by the Spanish Data Protection Agency, has adopted corrective measures aimed at putting an end to the possible breach of data protection legislation and any of the following circumstances apply:

a) That no harm has been caused to the affected party in the case of the infractions provided for in Article 74 of this Organic Law.

b) That the right of the affected party is fully guaranteed by the application of the measures.

4. Before deciding on the admissibility of the complaint, the Spanish Data Protection Agency may refer the same to the data protection officer who had, where appropriate, designated the controller or processor or to the supervisory body established for the implementation of codes of conduct for the purposes provided in Articles 37 and 38.2 of this Organic Law.

The Spanish Data Protection Agency may also refer the complaint to the data controller or processor when a data protection officer has not been appointed or has not adhered to out-of-court dispute resolution mechanisms, in which case the controller or processor must respond to the complaint within one month

5. The decision on the admission or rejection of the claim, as well as the decision determining, if applicable, the referral of the claim to the main supervisory authority deemed competent, shall be notified to the claimant within a period of three months. If this period has elapsed without such notification, it shall be understood that the processing of the complaint continues in accordance with the provisions of this Title as from the date on which three months have elapsed since the complaint was received by the Spanish Data Protection Agency.

Article 66. *Determination of the territorial scope.*

1. Except in the cases referred to in Article 64.3 of this Organic Law, the Spanish Data Protection Agency shall, prior to carrying out any other action, including the admission of a complaint for processing or the commencement of preliminary investigation actions, examine its competence and determine the national or cross-border nature, in any of its modalities, of the procedure to be followed.

2. If the Spanish Data Protection Agency considers that it does not have the status of main supervisory authority for the processing of the procedure, it will forward, without further formality, the claim formulated to the main supervisory authority that it considers competent, so that it may take the appropriate course of action. The Spanish Data Protection Agency shall notify this circumstance to the person who, as the case may be, had formulated the complaint.

The agreement resolving the referral referred to in the preceding paragraph shall imply the provisional filing of the proceedings, without prejudice to the Spanish Data Protection Agency issuing, if appropriate, the resolution referred to in Article 60(8) of Regulation (EU) 2016/679.

Article 67. *Preliminary investigative actions.*

1. Prior to the adoption of the resolution to initiate the procedure, and once the complaint has been admitted for processing, if any, the Spanish Data Protection Agency may carry out preliminary investigation actions in order to achieve a better determination of the facts and circumstances that justify the processing of the procedure.

The Spanish Data Protection Agency will act in any case when it is necessary to investigate processing operations involving massive traffic of personal data.

2. Preliminary investigation proceedings shall be subject to the provisions of Section 2 of Chapter I, Chapter I of Title VII of this Organic Law and may not have a duration of more than one year.

The Spanish Data Protection Agency acts on its own initiative or as a consequence of the communication sent to it by the supervisory authority of another Member State of the European Union, in accordance with Article 64.3 of this Organic Law, when the Spanish Data Protection Agency acts on its own initiative or as a consequence of the communication sent to it by the supervisory authority of another Member State of the European Union.

Article 68. *Agreement to initiate the procedure for the exercise of the sanctioning power.*

1. Once the proceedings referred to in the preceding article have been concluded, where appropriate, the Presidency of the Spanish Data Protection Agency shall be responsible for issuing a resolution to initiate proceedings for the exercise of the sanctioning authority, in which the facts, the identification of the person or entity against whom the proceedings are directed, the infringement that may have been committed and the possible sanction thereof shall be specified.

2. When the Spanish Data Protection Agency holds the status of lead supervisory authority and the procedure provided for in Article 60 of Regulation (EU) 2016/679 must be followed, the draft agreement to initiate the sanctioning procedure shall be subject to the provisions thereof.

Article 69. *Provisional measures and measures of guarantee of rights.*

1. During the performance of the preliminary investigation actions or the initiation of a procedure for the exercise of the sanctioning power, the Spanish Data Protection Agency may agree, with reasons, the necessary and proportionate provisional measures to safeguard the fundamental right to data protection and, in particular, those provided for in Article 66.1 of Regulation (EU) 2016/679, the precautionary blocking of the data and the immediate obligation to comply with the requested right.

2. In cases where the Spanish Data Protection Agency considers that the continued processing of personal data, their communication or international transfer would entail a serious undermining of the right to the protection of personal data, it may order data controllers or processors to block the data and cease their processing and, in the event of non-compliance with such orders, to immobilize them.

3. When a complaint has been filed with the Spanish Data Protection Agency that refers, among other issues, to the failure to comply with the rights established in Articles 15 to 22 of Regulation (EU) 2016/679 in due time, the Spanish Data Protection Agency may agree at any time, even prior to the initiation of the procedure for the exercise of the sanctioning power, by means of a reasoned resolution and after hearing the data controller, the obligation to comply with the right requested, continuing the procedure with respect to the rest of the issues that are the subject of the complaint.

TITLE IX

Penalty regime

Article 70. *Responsible parties.*

1. They are subject to the penalty regime established in Regulation (EU) 2016/679 and in this Organic Law:

a) Those responsible for the treatments.
b) The persons in charge of the treatments.
c) Representatives of controllers or processors not established in the territory of the European Union.
d) Certification entities.
e) Accredited entities for the supervision of codes of conduct.

2. The sanctioning regime established in this Title shall not apply to the data protection officer.

Article 71. *Infringements.*

The acts and conduct referred to in Article 83(4), (5) and (6) of Regulation (EU) 2016/679, as well as those that are contrary to this Organic Law, constitute infringements.

Article 72. *Violations considered very serious.*

1. According to the provisions of Article 83.5 of Regulation (EU) 2016/679, infringements involving a substantial violation of the articles mentioned therein and, in particular, the following are considered very serious and shall be subject to the statute of limitations after three years:

a) Processing personal data in breach of the principles and guarantees set out in Article 5 of Regulation (EU) 2016/679.
b) The processing of personal data without meeting any of the conditions for lawfulness of processing set out in Article 6 of Regulation (EU) 2016/679.

c) Failure to comply with the requirements required by Article 7 of Regulation (EU) 2016/679 for the validity of the consent.

d) The use of the data for a purpose that is not compatible with the purpose for which it was collected, without the consent of the data subject or a legal basis for it.

e) The processing of personal data of the categories referred to in Article 9 of Regulation (EU) 2016/679, without the occurrence of any of the circumstances provided for in that provision and in Article 9 of this Organic Law.

f) The processing of personal data relating to criminal convictions and offenses or related security measures outside the cases permitted by Article 10 of Regulation (EU) 2016/679 and in Article 10 of this Organic Law.

g) The processing of personal data related to administrative infractions and sanctions outside the cases permitted by article 27 of this Organic Law.

h) The omission of the duty to inform the data subject about the processing of his personal data in accordance with the provisions of Articles 13 and 14 of Regulation (EU) 2016/679 and 12 of this Organic Law.

i) Violation of the duty of confidentiality established in article 5 of this Organic Law.

j) The demand for payment of a fee for providing the data subject with the information referred to in Articles 13 and 14 of Regulation (EU) 2016/679 or for complying with requests for the exercise of rights of data subjects provided for in Articles 15 to 22 of Regulation (EU) 2016/679, outside the cases set forth in Article 12.5 thereof.

k) Impeding or hindering or repeatedly failing to exercise the rights set out in Articles 15 to 22 of Regulation (EU) 2016/679.

l) The international transfer of personal data to a recipient located in a third country or to an international organization, when the guarantees, requirements or exceptions set forth in Articles 44 to 49 of Regulation (EU) 2016/679 are not met.

m) Failure to comply with decisions issued by the competent data protection authority in exercise of the powers conferred on it by Article 58(2) of Regulation (EU) 2016/679.

n) Failure to comply with the obligation to block the data established in article 32 of this Organic Law when this obligation is enforceable.

ñ) Failure to provide the personnel of the competent data protection authority with access to personal data, information, premises, equipment and means of processing that are required by the data protection authority for the exercise of its investigative powers.

o) Resisting or obstructing the exercise of the inspection function by the competent data protection authority.

p) The deliberate reversal of an anonymization procedure in order to allow the re-identification of those concerned.

2. Infringements referred to in Article 83.6 of Regulation (EU) 2016/679 shall have the same consideration and shall also be subject to the statute of limitations after three years.

Article 73. *Violations considered serious.*

According to the provisions of Article 83.4 of Regulation (EU) 2016/679, infringements involving a substantial violation of the articles mentioned therein and, in particular, the following are considered serious and shall be subject to the statute of limitations after two years:

a) The processing of personal data of a minor without obtaining his or her consent, where he or she has the capacity to do so, or that of the holder of his or her parental authority or guardianship, in accordance with Article 8 of Regulation (EU) 2016/679.

b) Failure to demonstrate that reasonable efforts have been made to verify the validity of the consent given by a minor or by the holder of parental or guardianship rights.

guardianship over it, as required by Article 8.2 of Regulation (EU) 2016/679.

c) The hindrance or obstruction or repeated non-observance of the rights of access, rectification, erasure, limitation of processing or data portability in processing operations in which the identification of the data subject is not required, when the data subject, for the exercise of these rights, has provided additional information that allows his or her identification.

d) Failure to adopt those technical and organizational measures that are appropriate to effectively implement the principles of data protection by design, as well as failure to integrate the necessary safeguards in the processing, in the terms required by Article 25 of Regulation (EU) 2016/679.

e) Failure to take appropriate technical and organizational measures to ensure that, by default, only personal data necessary for each of the specific purposes of the processing will be processed, as required by Article 25(2) of Regulation (EU) 2016/679.

f) Failure to adopt those technical and organizational measures that are appropriate to ensure a level of security appropriate to the risk of the processing, in the terms required by Article 32.1 of Regulation (EU) 2016/679.

g) The breach, as a consequence of the lack of due diligence, of the technical and organizational measures that would have been implemented as required by Article 32.1 of Regulation (EU) 2016/679.

h) Failure to comply with the obligation to appoint a representative of the controller or processor not established in the territory of the European Union, as provided for in Article 27 of Regulation (EU) 2016/679.

i) Failure by the representative in the Union of the controller or processor to comply with requests made by the data protection authority or data subjects.

j) The hiring by the controller of a processor that does not provide sufficient guarantees to implement appropriate technical and organizational measures as set out in Chapter IV of Regulation (EU) 2016/679.

k) Entrust the processing of data to a third party without the prior formalization of a contract or other written legal act with the content required by Article 28.3 of Regulation (EU) 2016/679.

l) The contracting by a data processor of other data processors without the prior authorization of the data controller, or without having informed the data controller of the changes in the subcontracting when legally required.

m) Infringement by a processor of the provisions of Regulation (EU) 2016/679 and this Organic Law, when determining the purposes and means of processing, in accordance with the provisions of Article 28.10 of the aforementioned Regulation.

n) Not having the register of processing activities established in Article 30 of Regulation (EU) 2016/679.

ñ) Failure to make available to the data protection authority that has requested it, the register of processing activities, pursuant to Article 30(4) of Regulation (EU) 2016/679.

o) Failure to cooperate with the supervisory authorities in the performance of their duties in cases not provided for in Article 72 of this Organic Law.

p) The processing of personal data without carrying out a prior assessment of the elements mentioned in article 28 of this Organic Law.

q) Failure of the data processor to notify the data controller of security breaches of which it becomes aware.

r) Failure to comply with the duty to notify the data protection authority of a personal data security breach in accordance with the provisions of Article 33 of Regulation (EU) 2016/679.

s) Failure to notify the data subject of a data security breach in accordance with the provisions of Article 34 of the Regulation.

(EU) 2016/679 if the controller has been required by the data protection authority to carry out such notification.

t) The processing of personal data without having carried out the assessment of the impact of the processing operations on the protection of personal data in the cases in which it is required.

u) Processing personal data without prior consultation with the data protection authority in cases where such consultation is mandatory under Article 36 of Regulation (EU) 2016/679 or where the ley provides for the obligation to carry out such consultation.

v) Failure to comply with the obligation to appoint a data protection officer when his or her appointment is required in accordance with Article 37 of Regulation (EU) 2016/679 and Article 34 of this Organic Law.

w) Not enabling the effective participation of the data protection officer in all matters relating to the protection of personal data, not supporting him or her or interfering in the performance of his or her duties.

x) The use of a data protection seal or certification that has not been granted by a duly accredited certification body or if its validity has expired.

y) Obtaining accreditation as a certification body by submitting inaccurate information on compliance with the requirements required by Article 43 of Regulation (EU) 2016/679.

z) The performance of functions that Regulation (EU) 2016/679 reserves to certification bodies, without having been duly accredited in accordance with the provisions of Article 39 of this Organic Law.

aa) Failure by a certification body to comply with the principles and duties to which it is subject as provided for in Articles 42 and 43 of Regulation (EU) 2016/679.

(ab) Performing functions that Article 41 of Regulation (EU) 2016/679 reserves to code of conduct supervisory bodies without having been previously accredited by the competent data protection authority.

ac) Failure by the accredited supervisory bodies to adopt a code of conduct of the measures that are appropriate in the event that a breach of the code has occurred, as required by Article 41.4 of Regulation (EU) 2016/679.

Article 74. *Infractions considered minor.*

The remaining infringements of a purely formal nature of the Articles referred to in Article 83(4) and (5) of Regulation (EU) 2016/679, and in particular the following, shall be considered minor and shall be subject to the statute of limitations after one year:

a) Failure to comply with the principle of transparency of information or the data subject's right to information by not providing all the information required by Articles 13 and 14 of Regulation (EU) 2016/679.

b) The requirement of payment of a fee for providing the data subject with the information required by Articles 13 and 14 of Regulation (EU) 2016/679 or for complying with requests to exercise the rights of data subjects provided for in Articles 15 to 22 of Regulation (EU) 2016/679, when permitted by Article 12.5 thereof, if the amount exceeds the amount of the costs incurred in providing the information or carrying out the requested action.

c) Failure to respond to requests to exercise the rights set forth in Articles 15 to 22 of Regulation (EU) 2016/679, unless the provisions of Article 72.1.k) of this Organic Law apply.

d) Failure to comply with the rights of access, rectification, erasure, limitation of processing or data portability in processing operations where the identification of the data subject is not required, when the data subject, in order to exercise these rights, has provided the following information

additional information that allows their identification, unless the provisions of article 73 c) of this Organic Law apply.

e) Failure to comply with the notification obligation regarding rectification or erasure of personal data or restriction of processing required by Article 19 of Regulation (EU) 2016/679.

f) Failure to comply with the obligation to inform the data subject, when so requested, of the recipients to whom the rectified or deleted personal data have been communicated or in respect of whom processing has been restricted.

g) Failure to comply with the obligation to delete data referring to a deceased person when this is required in accordance with article 3 of this Organic Law.

h) The lack of formalization by the joint controllers of the agreement determining the respective obligations, roles and responsibilities with respect to the processing of personal data and their relations with data subjects referred to in Article 26 of Regulation (EU) 2016/679 or inaccuracy in the determination thereof.

i) Failure to make available to data subjects the essential aspects of the agreement formalized between the joint controllers of the processing, as required by Article 26.2 of Regulation (EU) 2016/679.

j) Failure to comply with the obligation of the processor to inform the controller about the possible infringement by an instruction received from the controller of the provisions of Regulation (EU) 2016/679 or of this Organic Law, as required by Article 28.3 of the aforementioned Regulation.

k) Failure by the processor to comply with the stipulations imposed in the contract or legal act regulating the processing or the instructions of the controller, unless it is legally obliged to do so in accordance with Regulation (EU) 2016/679 and this Organic Law or in cases where it was necessary to prevent the infringement of data protection legislation and the controller or the processor had been warned about it.

l) Having a Register of processing activities that does not incorporate all the information required by Article 30 of Regulation (EU) 2016/679.

m) Incomplete, late or defective notification to the data protection authority of information related to a personal data security breach in accordance with the provisions of Article 33 of Regulation (EU) 2016/679.

n) Failure to comply with the obligation to document any security breach, required by Article 33.5 of Regulation (EU) 2016/679.

ñ) Failure to comply with the duty to notify the data subject of a data security breach involving a high risk to the rights and freedoms of data subjects, as required by Article 34 of Regulation (EU) 2016/679, unless the provisions of Article 73 s) of this Organic Law apply.

o) Providing inaccurate information to the Data Protection Authority, in cases where the controller is required to submit a prior consultation to the Data Protection Authority, pursuant to Article 36 of Regulation (EU) 2016/679.

p) Not publishing the contact details of the data protection officer, or not communicating them to the data protection authority, when their appointment is required in accordance with Article 37 of Regulation (EU) 2016/679 and Article 34 of this Organic Law.

q) Failure by certification bodies to inform the data protection authority of the issuance, renewal or withdrawal of a certification, as required by Article 43(1) and (5) of Regulation (EU) 2016/679.

r) Failure by accredited supervisory bodies of a code of conduct to inform the data protection authorities of the measures that are appropriate in the event of a breach of the code, as required by Article 41(4) of Regulation (EU) 2016/679.

Article 75. *Interruption of the statute of limitations of the infringement.*

The prescription period shall be interrupted by the initiation, with the knowledge of the interested party, of the sanctioning procedure, and the prescription period shall be restarted if the sanctioning file has been paralyzed for more than six months for reasons not attributable to the alleged infringer.

When the Spanish Data Protection Agency holds the status of lead supervisory authority and the procedure provided for in Article 60 of Regulation (EU) 2016/679 must be followed, the statute of limitations shall be interrupted by the formal knowledge by the data subject of the draft commencement agreement that is submitted to the supervisory authorities concerned.

Article 76. *Sanctions and corrective measures.*

1. The penalties provided for in Article 83(4), (5) and (6) of Regulation (EU) 2016/679 shall be applied taking into account the graduation criteria set out in paragraph 2 of that Article.

2. In accordance with the provisions of Article 83.2.k) of Regulation (EU) 2016/679 they may also be taken into account:

a) The continuing nature of the infringement.

b) The link between the offender's activity and the processing of personal data.

c) The benefits obtained as a consequence of the commission of the infraction.

d) The possibility that the conduct of the person concerned could have induced the commission of the infringement.

e) The existence of a merger by absorption process subsequent to the commission of the infringement, which cannot be imputed to the absorbing entity.

f) Affectation of the rights of minors.

g) To have, when it is not mandatory, a data protection officer.

h) The submission by the person responsible or in charge, on a voluntary basis, to alternative dispute resolution mechanisms, in those cases in which there are disputes between them and any interested party.

3. It shall be possible, in addition or alternatively, the adoption, where appropriate, of the remaining corrective measures referred to in Article 83(2) of Regulation (EU) 2016/679.

4. Information identifying the infringer, the infringement committed and the amount of the sanction imposed shall be published in the Official State Gazette when the competent authority is the Spanish Data Protection Agency, the sanction exceeds one million euros and the infringer is a legal entity.

When the competent authority to impose the sanction is an autonomous data protection authority, its applicable regulations shall apply.

Article 77. *Regime applicable to certain categories of data controllers or processors.*

1. The regime established in this article shall apply to the processing operations for which they are responsible or in charge:

a) Constitutional bodies or bodies with constitutional relevance and the institutions of the autonomous communities analogous to them.

b) The jurisdictional bodies.

c) The General State Administration, the Administrations of the Autonomous Communities and the entities comprising the Local Administration.

d) Public bodies and public law entities linked to or dependent on the Public Administrations.

e) Independent administrative authorities.

f) The Bank of Spain.

g) Public law corporations when the purposes of the processing are related to the exercise of public law powers.

h) Public sector foundations.

i) Public Universities.

j) Consortiums.

k) The parliamentary groups of the Cortes Generales and the regional Legislative Assemblies, as well as the political groups of the Local Corporations.

2. When the persons responsible or in charge listed in paragraph 1 commit any of the infringements referred to in Articles 72 to 74 of this Organic Law, the competent data protection authority shall issue a decision sanctioning them with a warning. The resolution shall also establish the measures to be adopted in order to cease the conduct or to correct the effects of the infringement committed.

The resolution shall be notified to the person responsible for or in charge of the processing, to the body to which he/she reports hierarchically, if applicable, and to the affected parties who have the status of data subject, if applicable.

3. Without prejudice to the provisions of the preceding paragraph, the data protection authority shall also propose the initiation of disciplinary proceedings when there is sufficient evidence to do so. In this case, the procedure and sanctions to be applied will be those established in the applicable legislation on disciplinary or sanctioning regime.

Likewise, when the infractions are attributable to authorities and managers, and the existence of technical reports or recommendations for treatment that have not been duly attended to is accredited, the resolution imposing the sanction will include a warning with the name of the responsible position and will order its publication in the corresponding Official State or Autonomous Community Gazette.

4. The data protection authority must be notified of the resolutions passed in relation to the measures and actions referred to in the preceding paragraphs.

5. The Ombudsman or, as the case may be, the analogous institutions of the autonomous communities, shall be notified of the actions taken and the resolutions issued under this article.

6. When the competent authority is the Spanish Data Protection Agency, the latter shall publish on its web page, with due separation, the resolutions referring to the entities of paragraph 1 of this article, with express indication of the identity of the controller or data processor who has committed the infringement.

When the competence corresponds to an autonomous data protection authority, the publication of these resolutions shall be governed by the provisions of its specific regulations.

Article 78. *Prescription of penalties.*

1. Penalties imposed in application of Regulation (EU) 2016/679 and this Organic Law are subject to the following statute of limitations:

a) Penalties for amounts equal to or less than 40,000 euros are subject to a one-year statute of limitations.

b) Penalties of between 40,001 and 300,000 euros are subject to the statute of limitations. at two years of age.

c) Penalties of more than 300,000 euros are subject to a three-year statute of limitations.

2. The statute of limitations for penalties shall begin to run from the day following the day on which the resolution imposing the penalty becomes enforceable or the time limit for appealing it has elapsed.

3. The statute of limitations shall be interrupted by the initiation, with the knowledge of the interested party, of the enforcement procedure, and the period shall start to run again if the same is paralyzed for more than six months for reasons not attributable to the infringer.

TITLE X

Guarantee of digital rights

Article 79. *Rights in the Digital Age.*

The rights and freedoms enshrined in the Constitution and in the International Treaties and Conventions to which Spain is a party are fully applicable on the Internet. Information society service providers and Internet service providers shall contribute to guarantee their application.

Article 80. *Right to the neutrality of the Internet.*

Users have the right to Internet neutrality. Internet service providers shall provide a transparent offer of services without discrimination on technical or economic grounds.

Article 81. *Right to universal access to the Internet.*

1. Everyone has the right to access the Internet regardless of their personal, social, economic or geographic status.
2. Universal, affordable, quality and non-discriminatory access will be guaranteed for the entire population.
3. Internet access for men and women will help bridge the gender gap in both personal and work environments.
4. Internet access will seek to bridge the generation gap through actions aimed at training and access for the elderly.
5. The effective guarantee of the right to Internet access will take into account the specific reality of rural environments.
6. Internet access must guarantee equal conditions for people with special needs.

Article 82. *Right to digital security.*

Users have the right to the security of communications they transmit and receive over the Internet. Internet service providers shall inform users of their rights.

Article 83. *Right to digital education.*

1. The educational system will guarantee the full insertion of students in the digital society and the learning of a use of digital media that is safe and respectful of human dignity, constitutional values, fundamental rights and, particularly, respect and guarantee of personal and family privacy and the protection of personal data. The actions carried out in this area will be inclusive, particularly with regard to students with special educational needs.

The educational administrations must include in the design of the block of subjects of free configuration the digital competence referred to in the previous section, as well as the elements related to risk situations derived from the inadequate use of ICT, with special attention to situations of violence on the Internet.

2. Teachers shall receive the digital skills and training necessary for the teaching and transmission of the values and rights referred to in the previous section.

3. The curricula of university degrees, especially those that qualify students for professional training, shall guarantee training in the use and security of digital media and in the guarantee of fundamental rights on the Internet.

4. The Public Administrations shall incorporate subjects related to the guarantee of digital rights and, in particular, data protection, into the syllabus of the entrance exams to higher bodies and to those bodies in which functions involving access to personal data are usually performed.

Article 84. *Protection of minors on the Internet.*

1. Parents, guardians, tutors, curators or legal representatives shall ensure that minors make a balanced and responsible use of digital devices and information society services in order to guarantee the proper development of their personality and preserve their dignity and fundamental rights.

2. The use or dissemination of images or personal information of minors in social networks and equivalent information society services that may involve an unlawful interference in their fundamental rights will determine the intervention of the Public Prosecutor's Office, which will request the precautionary and protective measures provided for in Organic Law 1/1996, of January 15, 1996, on the Legal Protection of Minors.

Article 85. *Right of rectification on the Internet.*

1. Everyone has the right to freedom of expression on the Internet.

2. Those responsible for social networks and equivalent services shall adopt appropriate protocols to enable the exercise of the right of rectification by users who disseminate content that violates the right to honor, personal and family privacy on the Internet and the right to freely communicate or receive truthful information, in accordance with the requirements and procedures set forth in Organic Law 2/1984, of March 26, regulating the right of rectification.

When the digital media must comply with the request for rectification formulated against them, they must proceed to the publication in their digital archives of a clarifying notice stating that the original news item does not reflect the current situation of the individual. Said notice must appear in a visible place together with the original information.

Right to update information in digital media.

Any person has the right to request from the digital media the inclusion of a sufficiently visible update notice next to the news concerning him/her when the information contained in the original news item does not reflect his/her current situation as a consequence of circumstances that have occurred after the publication, causing him/her a prejudice.

In particular, the inclusion of such a notice shall be appropriate when the original information relates to police or judicial proceedings that have been affected for the benefit of the data subject as a result of subsequent judicial decisions. In this case, the notice shall refer to the subsequent decision.

Article 87. *Right to privacy and use of digital devices in the workplace.*

1. Workers and public employees shall have the right to protection of their privacy in the use of digital devices made available to them by their employer.

2. The employer may access the contents derived from the use of digital media provided to workers for the sole purpose of monitoring compliance with labor or statutory obligations and ensuring the integrity of such devices.

3. Employers must establish criteria for the use of digital devices, respecting in all cases the minimum standards for the protection of their privacy in accordance with social uses and the rights recognized constitutionally and legally. Workers' representatives must participate in its development.

Access by the employer to the content of digital devices for which the employer has admitted their use for private purposes shall require that the authorized uses are precisely specified and that safeguards are established to preserve the privacy of workers, such as, where appropriate, the determination of the periods during which the devices may be used for private purposes.

Workers shall be informed of the criteria for use referred to in this section.

Article 88. *Right to digital disconnection in the workplace.*

1. Public workers and employees shall have the right to digital disconnection in order to guarantee, outside the legally or conventionally established working time, respect for their rest, leave and vacation time, as well as their personal and family privacy.

2. The modalities for exercising this right shall take into account the nature and purpose of the employment relationship, shall promote the right to reconcile work and personal and family life, and shall be subject to the provisions of collective bargaining or, failing this, to the agreement between the company and the workers' representatives.

3. The employer, after hearing the workers' representatives, shall draw up an internal policy aimed at workers, including those in managerial positions, defining the modalities for exercising the right to disconnection and the training and awareness-raising actions for personnel on the reasonable use of technological tools to avoid the risk of computer fatigue. In particular, the right to digital disconnection will be preserved in cases of total or partial remote work and at the employee's home in connection with the use of technological tools for work purposes.

Right to privacy against the use of video surveillance and sound recording devices in the workplace.

1. Employers may process the images obtained through camera or video camera systems for the exercise of the functions of control of workers or public employees provided, respectively, in Article 20.3 of the Workers' Statute and in the civil service legislation, provided that these functions are exercised within their legal framework and with the limits inherent thereto. Employers shall inform in advance, and in an express, clear and concise manner, the workers or public employees and, where appropriate, their representatives, about this measure.

In the event that the flagrant commission of an unlawful act by workers or public employees has been detected, the duty to report shall be deemed to have been fulfilled when there is at least the device referred to in Article 22.4 of this Organic Law.

2. In no case shall the installation of sound recording or video surveillance systems be allowed in places intended for the rest or recreation of workers or public employees, such as changing rooms, toilets, dining rooms and the like.

3. The use of systems similar to those referred to in the previous sections for the recording of sounds in the workplace will only be allowed when the risks to the safety of the installations, goods and persons derived from the activity carried out in the workplace are relevant and always respecting the principle of proportionality, the principle of minimum intervention and the guarantees provided for in the previous sections. The suppression of the sounds preserved by these recording systems shall be carried out in accordance with the provisions of section 3 of article 22 of this Law.

code: BO-EA- 201-8 16673
Verifiable at http ://www.boe.es

Article 90. *Right to privacy in the use of geolocation systems in the workplace.*

1. Employers may process data obtained through geolocation systems for the exercise of the functions of control of workers or public employees provided, respectively, in Article 20.3 of the Workers' Statute and in the civil service legislation, provided that these functions are exercised within their legal framework and with the limits inherent to it.

2. Beforehand, employers must expressly, clearly and unequivocally inform workers or public employees and, where appropriate, their representatives, about the existence and characteristics of these devices. They must also inform them about the possible exercise of the rights of access, rectification, limitation of processing and erasure.

Article 91. *Digital rights in collective bargaining.*

Collective bargaining agreements may provide for additional guarantees of rights and freedoms related to the processing of workers' personal data and the safeguarding of digital rights in the workplace.

Article 92. *Data protection of minors on the Internet.*

Educational centers and any natural or legal persons that carry out activities involving minors shall ensure the protection of the best interests of minors and their fundamental rights, especially the right to the protection of personal data, in the publication or dissemination of their personal data through information society services.

When such publication or dissemination were to take place through social networking services or equivalent services must have the consent of the minor or their legal representatives, as prescribed in Article 7 of this organic law.

Article 93. *Right to be forgotten in Internet searches.*

1. Every person has the right to have Internet search engines remove from the lists of results obtained after a search carried out on the basis of his or her name any published links containing information relating to that person when they are inadequate, inaccurate, irrelevant, outdated or excessive or have become so over time, taking into account the purposes for which they were collected or processed, the time that has elapsed and the nature and public interest of the information.

The same procedure shall be followed when the personal circumstances invoked by the affected party show the prevalence of his rights over the maintenance of the links by the Internet search service.

This right shall subsist even if the information published on the website to which the link is directed is unlawfully retained and is not deleted before or at the same time.

2. The exercise of the right referred to in this article shall not prevent access to the information published on the website through the use of search criteria other than the name of the person exercising the right.

Article 94. *Right to be forgotten in social networking services and equivalent services.*

1. Any person has the right to have personal data that he/she has provided for publication by social networking services and equivalent information society services deleted upon simple request.

2. Everyone has the right to the deletion of personal data concerning him or her that has been provided by third parties for publication by the

code: BO-EA- 201-8 16673
Verifiable at http ://www.boe.es

social networking services and equivalent information society services when they are inadequate, inaccurate, irrelevant, outdated or excessive or have become so over time, taking into account the purposes for which they were collected or processed, the time that has elapsed and the nature and public interest of the information.

In the same way, such data shall be deleted when the personal circumstances invoked by the affected party show the prevalence of his rights over the maintenance of the data by the service.

Exceptions to the provisions of this paragraph are data provided by individuals in the exercise of personal or domestic activities.

3. In the event that the right is exercised by a data subject with respect to data that have been provided to the service, by him or by third parties, during his minority, the provider shall proceed without delay to their deletion upon his simple request, without the need for the circumstances mentioned in paragraph 2 to be met.

Article 95. *Right of portability in social network services and equivalent services.*

Users of social networking services and equivalent information society services shall have the right to receive and transmit the contents they have provided to the providers of such services, as well as to have the providers transmit them directly to another provider designated by the user, provided that it is technically possible.

Providers may retain, without disseminating it over the Internet, a copy of the contents when such retention is necessary to comply with a legal obligation.

Article 96. *Right to a digital will.*

1. Access to content managed by information society service providers about deceased persons shall be governed by the following rules:

a) Persons related to the deceased for family or de facto reasons, as well as their heirs, may contact the information society service providers in order to access such content and give them the instructions they deem appropriate regarding its use, destination or deletion.

As an exception, the aforementioned persons may not access the contents of the deceased, nor request their modification or elimination, when the deceased had expressly forbidden it or when it is so established by law. Such prohibition shall not affect the right of the heirs to access the contents that may form part of the estate.

b) The executor of the will, as well as any person or institution expressly designated by the deceased, may also request, in accordance with the instructions received, access to the contents in order to comply with such instructions.

c) In the case of deceased minors, these powers may also be exercised by their legal representatives or, within the framework of its competencies, by the Public Prosecutor's Office, which may act ex officio or at the request of any interested individual or legal entity.

d) In the event of death of persons with disabilities, these powers may also be exercised, in addition to those mentioned in the preceding paragraph, by those who have been designated to perform support functions if such powers are understood to be included in the support measures provided by the designated person.

2. The persons entitled in the previous paragraph may decide on the maintenance or elimination of personal profiles of deceased persons in networks.

The deceased will be entitled to social security or equivalent services, unless the deceased had decided about this circumstance, in which case his or her instructions will be followed.

The person in charge of the service who is notified, in accordance with the previous paragraph, of the request for removal of the profile, shall proceed without delay to do so.

3. A Royal Decree shall establish the requirements and conditions for accrediting the validity and validity of the mandates and instructions and, as the case may be, their registration, which may coincide with that provided for in Article 3 of this Organic Law.

4. The provisions of this article in relation to persons deceased in the autonomous communities with their own civil, foral or special law shall be governed by the provisions of these communities within their scope of application.

Article 97. *Policies for the promotion of digital rights.*

1. The Government, in collaboration with the autonomous communities, will prepare an Internet Access Plan with the following objectives:

a) overcoming the digital divide and guaranteeing Internet access for vulnerable groups or those with special needs and from economically disadvantaged family and social environments through, among other measures, a social voucher for Internet access;

b) promoting the existence of publicly accessible connecting spaces; and

c) to encourage educational measures that promote training in basic digital competencies and skills for people and groups at risk of digital exclusion and the ability of all people to make autonomous and responsible use of the Internet and digital technologies.

2. Likewise, an Action Plan will be approved aimed at promoting the necessary training, dissemination and awareness-raising actions to ensure that minors make a balanced and responsible use of digital devices and social networks and the equivalent information society services of the Internet in order to guarantee their adequate development of their personality and to preserve their dignity and fundamental rights.

3. The Government shall submit an annual report to the corresponding parliamentary committee of the Congress of Deputies in which it shall give an account of the evolution of the rights, guarantees and mandates contemplated in this Title and of the measures necessary to promote their momentum and effectiveness.

First additional provision. *Security measures in the public sector.*

1. The National Security Scheme shall include the measures to be implemented in case of processing of personal data to prevent their loss, alteration or unauthorized access, adapting the criteria for determining the risk in the processing of data to the provisions of Article 32 of Regulation (EU) 2016/679.

2. The controllers listed in Article 77.1 of this Organic Law must apply to the processing of personal data the security measures that correspond to those provided for in the National Security Scheme, as well as promote a degree of implementation of equivalent measures in companies or foundations linked to them subject to private law.

In cases where a third party provides a service under a concession, management assignment or contract, the security measures shall correspond to those of the originating public administration and shall comply with the National Security Scheme.

Second additional provision: *Data protection and transparency and access to public information.*

Active publicity and access to public information regulated by Title I of Law 19/2013, of December 9, 2013, on transparency, access to public information and good governance.

government, as well as the active publicity obligations established by regional legislation, shall be subject, when the information contains personal data, to the provisions of Articles 5.3 and 15 of Law 19/2013, Regulation (EU) 2016/679 and this Organic Law.

Third additional provision. *Computation of deadlines.*

The time limits established in Regulation (EU) 2016/679 or in this Organic Law, regardless of whether they refer to relations between individuals or with public sector entities, shall be governed by the following rules:

a) When deadlines are indicated in days, it is understood that these are working days, excluding Saturdays, Sundays and declared holidays.

b) If the term is fixed in weeks, it will end on the same day of the week in which it is fixed. the event that determines its initiation occurred in the expiration week.

c) If the term is fixed in months or years, it shall end on the same day on which the event that determines its initiation in the month or year of expiration occurred. If in the month of expiration there is no day equivalent to that on which the computation begins, it shall be understood that the term expires on the last day of the month.

d) When the last day of the period is a non-business day, it shall be understood to be extended to the first following business day.

Fourth additional provision. *Procedure in relation to the powers attributed to the Spanish Data Protection Agency by other laws.*

The provisions of Title VIII and its implementing regulations shall be applicable to the procedures that the Spanish Data Protection Agency may have to process in the exercise of the powers attributed to it by other laws.

Fifth additional provision. *Judicial authorization in relation to decisions of the European Commission on international data transfer.*

1. Where a data protection authority considers that a decision of the European Commission on the international transfer of data, on the validity of which the outcome of a specific procedure depends, infringes the provisions of Regulation (EU) 2016/679, undermining the fundamental right to data protection, it shall immediately agree to suspend the procedure, in order to request authorization from the judicial body to declare it so in the proceedings before it. Such suspension shall be confirmed, modified or lifted in the decision to admit or refuse to admit the request of the data protection authority addressed to the competent court.

The decisions of the European Commission to which this channel may be applicable are as follows:

a) those declaring the adequate level of protection of a third country or international organization, pursuant to Article 45 of Regulation (EU) 2016/679;

b) those approving standard data protection clauses for international data transfers, or

c) those that declare the validity of the codes of conduct to that effect.

2. The authorization referred to in this provision may only be granted if, after a preliminary ruling on the validity of the decision of the European Commission, as provided for in Article 267 of the Treaty on the Functioning of the European Union, the decision of the European Commission in question is declared invalid by the Court of Justice of the European Union.

Sixth additional provision: *Incorporation of debts to credit information systems.*

The credit information systems referred to in Article 20.1 of this Organic Law shall not include debts in which the principal amount is less than fifty euros.

The Government, by Royal Decree, may update this amount.

Seventh additional provision. *Identification of interested parties in notifications by means of announcements and publications of administrative acts.*

1. When the publication of an administrative act containing personal data of the affected party is necessary, the affected party shall be identified by his or her name and surname, adding four random numerical digits of the national identity card, foreigner's identity number, passport or equivalent document. When the publication refers to a plurality of affected persons, these random digits must be alternated.

In the case of notification by means of notices, particularly in the cases referred to in Article 44 of Law 39/2015, of October 1, of the Common Administrative Procedure of Public Administrations, the affected party shall be identified exclusively by means of the full number of their national identity document, foreigner's identity number, passport or equivalent document.

When the affected person lacks any of the documents mentioned in the two preceding paragraphs, the affected person will be identified only by his or her name and surname. In no case shall the name and surname be published together with the full number of the national identity document, foreigner's identity number, passport or equivalent document.

2. In order to prevent risks for victims of gender violence, the Government will promote the elaboration of a collaboration protocol that defines safe procedures for the publication and notification of administrative acts, with the participation of the bodies with competence in the matter.

Eighth Additional Provision. *Verification powers of the Public Administrations.*

When requests are made by any means in which the interested party declares personal data held by the Public Administrations, the body to which the request is addressed may, in the exercise of its powers, carry out the necessary verifications to check the accuracy of the data.

Ninth additional provision. *Processing of personal data in relation to the notification of security incidents.*

When, in accordance with the provisions of the applicable national legislation, security incidents must be notified, the competent public authorities, computer emergency response teams (CERT), computer security incident response teams (CSIRT), providers of electronic communications networks and services and providers of security technologies and services, may process the personal data contained in such notifications, exclusively for the time and scope necessary for their analysis, detection, protection and response to incidents and adopting the appropriate security measures proportionate to the determined level of risk.

Tenth additional provision. *Communications of data by the parties listed in article 77.1.*

The data controllers listed in Article 77.1 of this Organic Law may communicate the personal data requested by private law entities when they have the consent of the data subjects or when they consider that the data subjects are in the possession of the data subjects.

applicants a legitimate interest that prevails over the rights and interests of those affected as set out in Article 6(1)(f) of Regulation (EU) 2016/679.

Eleventh additional provision. *Privacy in electronic communications.*

The provisions of this Organic Law shall be without prejudice to the application of the rules of domestic and European Union law governing privacy in the electronic communications sector, without imposing additional obligations on natural or legal persons regarding processing in the framework of the provision of public electronic communications services in public communications networks in areas in which they are subject to specific obligations established in such rules.

Twelfth additional provision: *Specific provisions applicable to the processing of public sector personnel records.*

1. Processing of public sector personnel records shall be understood to be carried out in the exercise of public powers vested in the persons in charge thereof, in accordance with the provisions of Article 6(1)(e) of Regulation (EU) 2016/679.
2. Public sector personnel registries may process personal data relating to criminal offenses and convictions and administrative offenses and penalties, limited to the data strictly necessary for the fulfillment of their purposes.
3. In accordance with the provisions of Article 18(2) of Regulation (EU) 2016/679, and because it is considered a reason of substantial public interest, data whose processing has been restricted under Article 18(1) of the aforementioned regulation may be processed when necessary for the performance of personnel procedures.

Thirteenth additional provision. *International transfers of tax data.*

Transfers of tax data between the Kingdom of Spain and other States or international or supranational entities shall be regulated by the terms and within the limits established in the regulations on mutual assistance between the States of the European Union, or within the framework of agreements to avoid double taxation or other international agreements, as well as by the rules on mutual assistance established in Chapter VI of Title III of Law 58/2003, of December 17, 2003, General Tax Law.

Fourteenth additional provision. *Rules issued in development of Article 13 of Directive 95/46/EC.*

The rules issued in application of Article 13 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which had entered into force prior to May 25, 2018, and in particular Articles 23 and 24 of Organic Law 15/1999 of December 13 on the Protection of Personal Data, remain in force as long as they are not expressly amended, replaced or repealed.

Fifteenth Additional Provision. *Request for information by the National Securities Market Commission.*

When it has not been able to obtain by other means the information necessary to carry out its supervision or inspection tasks, the National Securities Market Commission may request from the operators that provide electronic communications services available to the public and from the providers of information society services, the data in its possession relating to the electronic communication or information society service provided by said providers that are different from their content and are essential for the exercise of said tasks.

The transfer of such data shall require prior judicial authorization granted in accordance with the procedural rules.

Excluded from the provisions of this section are traffic data that operators are processing for the sole purpose of complying with the obligations set forth in Law 25/2007, of October 18, 2007, on the conservation of data relating to electronic communications and public communications networks.

Sixteenth additional provision. *Aggressive data protection practices.*

For the purposes set forth in Article 8 of Law 3/1991, of January 10, 1991, on Unfair Competition, the following are considered aggressive practices:

a) Acting with intent to impersonate the Spanish Data Protection Agency or an autonomous data protection authority when making any communication to data controllers, data processors or data subjects.

b) Generate the appearance of acting in the name of, on behalf of or in collaboration with the Spanish Data Protection Agency or an autonomous data protection authority when making any communication to the data controllers and data processors in which the sender offers its products or services.

c) Engaging in commercial practices that restrict the decision-making power of recipients by referring to the possible imposition of penalties for non-compliance with personal data protection regulations.

d) Offering any type of document intended to create the appearance of compliance with data protection provisions in addition to the implementation of training activities without having carried out the necessary actions to verify that such compliance actually occurs.

e) To assume, without express designation of the data controller or data processor, the function of data protection officer and to communicate in such capacity with the Spanish Data Protection Agency or the autonomous data protection authorities.

Seventeenth additional provision. *Treatment of health data.*

1. Covered by Article 9(2)(g), (h), (i) and (j) of Regulation (EU) 2016/679 are the processing of health-related data and genetic data that are regulated by the following laws and their implementing provisions:

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

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

c) Law 41/2002, of November 14, 2002, basic law regulating patient autonomy and the rights and obligations regarding clinical information and documentation.

d) Law 16/2003, of May 28, 2003, on the cohesion and quality of the National Health System.

e) Law 44/2003, of November 21, 2003, on the regulation of health professions.

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

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

h) Law 20/2015, of July 14, on the regulation, supervision and solvency of insurance and reinsurance companies.

i) The revised text of the Law on Guarantees and Rational Use of Medicines and Medical Devices, approved by Royal Legislative Decree 1/2015, of July 24, 2015.

j) The revised text of the General Law on the Rights of Persons with Disabilities and their Social Inclusion, approved by Royal Legislative Decree 1/2013 of November 29.

2. Data processing in health research will be governed by the following criteria:

a) The data subject or, where appropriate, his or her legal representative may consent to the use of his or her data for health research purposes and, in particular, biomedical research. Such purposes may include categories related to general areas linked to a medical or research specialty.

b) Health authorities and public institutions with competences in public health surveillance may carry out scientific studies without the consent of those affected in situations of exceptional relevance and seriousness for public health.

c) The reuse of personal data for health and biomedical research purposes will be considered lawful and compatible when, having obtained consent for a specific purpose, the data are used for purposes or areas of research related to the area in which the initial study was scientifically integrated.

In such cases, the responsible parties must publish the information established by Article 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of their personal data and on the free movement of such data, in an easily accessible place on the corporate website of the center where the research or clinical study is conducted, and, where appropriate, on that of the sponsor, and notify the existence of this information by electronic means to those affected. When they do not have the means to access such information, they may request that it be sent in another format.

For the treatments foreseen in this letter, a prior favorable report from the research ethics committee shall be required.

d) The use of pseudonymized personal data for health and, in particular, biomedical research purposes is considered lawful.

The use of pseudonymized personal data for public health and biomedical research purposes will require:

1.° A technical and functional separation between the research team and those who perform the pseudonymization and keep the information that makes re-identification possible.

2.° Pseudonymized data should only be accessible to the research team when:

i) There is an express commitment to confidentiality and not to engage in any re-identification activity.

ii) Specific security measures are adopted to prevent re-identification and access by unauthorized third parties.

Data may be re-identified at source when, in the course of an investigation using pseudonymized data, there is a real and concrete danger to the safety or health of a person or group of persons, or a serious threat to their rights, or it is necessary to ensure adequate health care.

e) Where personal data are processed for the purposes of health research, and in particular biomedical research, for the purposes of Article 89(2) of Regulation (EU) 2016/679, the rights of data subjects provided for in Articles 15, 16, 18 and 21 of Regulation (EU) 2016/679 may be waived where:

1.The aforementioned rights are exercised directly against researchers or research centers using anonymized or pseudonymized data.

2.° The exercise of such rights refers to the results of the research.

3.° The investigation has as its object an essential public interest related to the security of the State, defense, public safety or other important objectives of general public interest, provided that in the latter case the exception is expressly provided for by a regulation with the rank of Law.

f) When, in accordance with the provisions of Article 89 of Regulation (EU) 2016/679, processing is carried out for the purposes of public health research and, in particular, biomedical research, the following shall be carried out:

1.° Conduct an impact assessment identifying the risks arising from the processing in the cases provided for in Article 35 of Regulation (EU) 2016/679 or those established by the supervisory authority. This assessment shall specifically include the re-identification risks linked to the anonymization or pseudonymization of data.

2.° To subject scientific research to quality standards and, where appropriate, to international guidelines on good clinical practice.

3.° Adopt, where appropriate, measures to ensure that researchers do not have access to identification data of the interested parties.

4.° Designate a legal representative established in the European Union, in accordance with Article 74 of Regulation (EU) 536/2014, if the sponsor of a clinical trial is not established in the European Union. Such legal representative may coincide with the one provided for in Article 27(1) of Regulation (EU) 2016/679.

g) The use of pseudonymized personal data for public health and, in particular, biomedical research purposes must be subject to the prior report of the research ethics committee provided for in the sectoral regulations.

In the absence of the existence of the aforementioned Committee, the entity responsible for the investigation shall require prior report from the data protection officer or, failing that, from an expert with the prior knowledge in Article 37.5 of Regulation (EU) 2016/679.

h) No later than one year after the entry into force of this ley, research ethics committees, in the health, biomedical or drug field, must integrate among their members a data protection officer or, failing that, an expert with sufficient knowledge of Regulation (EU) 2016/679 when dealing with research activities involving the processing of personal data or pseudonymized or anonymized data.

Eighteenth additional provision. *Safety criteria.*

The Spanish Data Protection Agency will develop, with the collaboration, when necessary, of all the actors involved, the tools, guides, guidelines and orientations that are necessary to provide professionals, micro, small and medium-sized companies with appropriate guidelines for compliance with the obligations of active responsibility established in Title IV of Regulation (EU) 2016/679 and in Title V of this Organic Law.

Nineteenth additional provision. *Rights of minors before the Internet.*

Within one year of the entry into force of this organic law, the Government shall submit to the Congress of Deputies a draft law specifically aimed at guaranteeing the rights of minors in the face of the impact of the Internet, in order to ensure their safety and fight against discrimination and violence against them through new technologies.

Twentieth Additional Provision. *Specialties of the legal regime of the Spanish Data Protection Agency.*

1. The Spanish Data Protection Agency shall not be subject to the provisions of Article 50.2.c) of Law 40/2015, of October 1, of the Public Sector Legal Regime.

2. The Spanish Data Protection Agency may adhere to the centralized contracting systems established by the Public Administrations and may participate in the

shared management of common services provided for in Article 85 of Law 40/2015, of October 1, of the Public Sector Legal Regime.

Twenty-first additional provision. *Digital education.*

The educational Administrations shall comply with the mandate contained in the second paragraph of section 1 of article 83 of this Organic Law within one year of its entry into force.

Twenty-second additional provision. *Access to public and ecclesiastical archives.*

The competent public authorities shall facilitate access to public and ecclesiastical archives in relation to data requested in connection with police or judicial investigations of missing persons, and requests shall be dealt with promptly and diligently by the religious institutions or congregations to which the requests for access are made.

First Transitory Provision. *Statute of the Spanish Data Protection Agency.*

1. The Statute of the Spanish Data Protection Agency, approved by Royal Decree 428/1993, of March 26, 1993, shall remain in force insofar as it does not oppose the provisions of Title VIII of this Organic Law.

2. The provisions of paragraphs 2, 3 and 5 of Article 48 and Article 49 of this Organic Law shall apply once the term of office of the person holding the position of Director of the Spanish Data Protection Agency on the entry into force of the same has expired.

Second Transitory Provision. *Standard codes registered with the data protection authorities in accordance with Organic Law 15/1999, of December 13, 1999, on the Protection of Personal Data.*

The promoters of the standard codes registered in the registry of the Spanish Data Protection Agency or in the regional data protection authorities must adapt their content to the provisions of Article 40 of Regulation (EU) 2016/679 within one year from the entry into force of this Organic Law.

If, after said period has elapsed, the approval provided for in Article 38.4 of this Organic Law has not been requested, the registration shall be cancelled and the promoters shall be notified.

Third Transitory Provision. *Transitory regime of the procedures.*

1. Proceedings already initiated upon the entry into force of this Organic Law shall be governed by the previous regulations, unless this Organic Law contains provisions that are more favorable to the interested party.

2. The provisions of the preceding paragraph shall also apply to the proceedings in respect of which the preliminary proceedings referred to in Section 2a of Chapter III of Title IX of the implementing regulations have already been initiated.
of the Organic Law 15/1999, of December 13, 1999, on the Protection of Personal Data, approved by Royal Decree 1720/2007, of December 21, 2007.

Transitional provision four. *Treatments subject to Directive (EU) 2016/680.*

Processing operations subject to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA, shall continue to be governed by Organic Law 15/1999 of 13 December, and in particular Article 22 and its provisions.

The Company has not yet entered into force the regulations transposing the provisions of the aforementioned directive into Spanish law.

Fifth transitory provision. *Contracts of data processor.*

The data processor contracts signed prior to May 25, 2018 under the provisions of Article 12 of Organic Law 15/1999, of December 13, 1999, on the Protection of Personal Data shall remain in force until the expiration date indicated therein and, in the event that they have been agreed indefinitely, until May 25, 2022.

During such periods either party may require the other party to amend the contract in order to bring the contract into conformity with the provisions of Article 28 of Regulation (EU) 2016/679 and Chapter II of Title V of this Organic Law.

Sixth transitional provision. *Reuse for health and biomedical research purposes of personal data collected prior to the entry into force of this Organic Law.*

The reuse for health and biomedical research purposes of personal data collected prior to the entry into force of this Organic Law shall be considered lawful and compatible when any of the following circumstances apply:

a) That such personal data is used for the specific purpose for which consent was given.

b) That, having obtained consent for a specific purpose, such data be used for purposes or areas of research related to the medical or research specialty in which the initial study was scientifically integrated.

Sole derogatory provision. *Repeal of regulations.*

1. Without prejudice to the provisions of the fourteenth additional provision and the fourth transitory provision, Organic Law 15/1999, of December 13, 1999, on the Protection of Personal Data is hereby repealed.

2. Royal Decree-Law 5/2018 of July 27, 2018, on urgent measures for the adaptation of Spanish law to European Union regulations on data protection is hereby repealed.

3. Likewise, any provisions of equal or lower rank that contradict, oppose or are incompatible with the provisions of Regulation (EU) 2016/679 and this Organic Law are hereby repealed.

First final provision. *Nature of this law.*

The present law has the character of an organic law.

However, they have the character of ordinary laws:

– Title IV,
– Title VII, except for Articles 52 and 53, which are of an organic nature,
– Title VIII,
– Title IX,
— articles 79, 80, 81, 82, 88, 95, 96 and 97 of Title X,
– the additional provisions, except for the second additional provision and the seventeenth additional provision, which are of an organic nature,
– transitional provisions,
– and the final provisions, except for the first, second, third, fourth, eighth, tenth and sixteenth final provisions, which are of an organic nature.

code: BO-EA- 201-8 16673
Verifiable at http ://www.boe.es

Second final provision. *Competent title.*

1. This organic law is enacted under Article 149.1.1.1 á of the Constitution, which attributes to the State the exclusive competence for the regulation of the basic conditions that guarantee the equality of all Spaniards in the exercise of their rights and in the fulfillment of their constitutional duties.

2. Chapter I of Title VII, Title VIII, the fourth additional provision and the first transitory provision shall only apply to the General State Administration and its public agencies.

3. Articles 87 to 90 are enacted under the exclusive competence that Article 149.1.7 and 18 of the Constitution reserves to the State in the area of legislation.
and bases of the statutory regime for civil servants, respectively.

4. The fifth additional provision and the seventh and sixth final provisions are issued under the competence that Article 149.1.6 á of the Constitution attributes to the State.
in procedural law.

5. The third additional provision is issued under Article 149.1.18 á of the Constitution.

6. Article 96 is enacted under Article 149.1.8 á of the Constitution.

Third final provision: *Amendment of Organic Law 5/1985, of June 19, 1985, on the General Electoral System.*

Organic Law 5/1985, of June 19, 1985, on the General Electoral System is amended to read as follows:

Paragraph 3 of article thirty-nine shall read as follows:

"Within the aforementioned period, any person may file a complaint addressed to the Provincial Delegation of the Electoral Census Office regarding their census data, although only those that refer to the rectification of errors in personal data, changes of address within the same district or the non-inclusion of the claimant in any Census Section of the district despite being entitled to it, may be taken into account. The requests of voters who object to their inclusion in the copies of the electoral roll that are provided to the representatives of the candidacies for the purpose of sending electoral propaganda mailings shall also be considered. Those reflecting a change of residence from one constituency to another, made after the closing date of the census for each election, shall not be taken into account for the election summoned, and they shall exercise their right in the section corresponding to their previous domicile."

A new article fifty-eight bis is hereby added, with the following content:

"Article fifty-eight bis. *Use of technological means and personal data in electoral activities.*

1. The collection of personal data relating to the political opinions of individuals carried out by political parties in the framework of their electoral activities shall be covered by the public interest only when adequate safeguards are provided.

2. Political parties, coalitions and electoral groups may use personal data obtained from web pages and other publicly accessible sources for the performance of political activities during the electoral period.

3. The sending of electoral propaganda by electronic means or messaging systems and the contracting of electoral propaganda in social networks or equivalent media shall not be considered as a commercial activity or communication.

4. The aforementioned dissemination activities shall prominently identify their electoral nature.

5. The addressee shall be provided with a simple and free way of exercising the right to object."

Fourth final provision: *Amendment of Organic Law 6/1985, of July 1, 1985, of the Judiciary.*

Organic Law 6/1985, of July 1, 1985, of the Judiciary is amended as follows:

A third paragraph is added to Article 58, with the following wording:

"Article 58.

Third. Of the request for authorization for the declaration provided for in the fifth additional provision of the Organic Law on Personal Data Protection and Guarantee of Digital Rights, when such request is made by the General Council of the Judiciary."

Two.A letter f) is added to Article 66, with the following wording:

"Article 66.

f) Of the request for authorization for the declaration provided for in the fifth additional provision of the Organic Law on Personal Data Protection and Guarantee of Digital Rights, when such request is made by the Spanish Data Protection Agency."

Three. A letter k) is added to paragraph 1 and a new paragraph 7 to Article 74, with the following wording:

"Article 74.

1. [...]

k) The request for authorization for the declaration provided for in the fifth additional provision of the Organic Law on Personal Data Protection and Guarantee of Digital Rights, when such request is made by the data protection authority of the respective Autonomous Community.

7. The Contentious-Administrative Chambers of the High Courts of Justice shall be responsible for authorizing, by means of an order, the request for information by the autonomous data protection authorities to operators providing publicly available electronic communications services and providers of information society services, when this is necessary in accordance with specific legislation".

A new paragraph 7 is added to Article 90:

"7. The Central Contentious-Administrative Courts shall be responsible for authorizing, by means of an order, the request for information by the Spanish Data Protection Agency and other independent administrative authorities at the state level to operators providing publicly available electronic communications services and providers of information society services, when this is necessary in accordance with specific legislation."

Fifth final provision: *Modification of Law 14/1986, of April 25, 1986, General Health Law.*

A new Chapter II is added to Title VI of Law 14/1986, of April 25, 1986, General Health Law, with the following content:

"CHAPTER II

Treatment of health research data

Article 105 bis.

The processing of personal data in health research will be governed by the provisions of the seventeenth additional provision of the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights."

Sixth final provision: *Modification of Law 29/1998, of July 13, 1998, regulating the Contentious-Administrative Jurisdiction.*

Law 29/1998, of July 13, 1998, regulating the Contentious-Administrative Jurisdiction, is amended as follows:

A new paragraph 7 is added to Article 10:

"7. They shall hear the request for authorization under Article 122 ter, when it is formulated by the data protection authority of the respective Autonomous Community."

Two. A new paragraph 5 is added to Article 11:

"5. It shall hear the request for authorization under Article 122 ter, when formulated by the Spanish Data Protection Agency."

A new paragraph 4 is added to Article 12:

"4. It shall hear the request for authorization under Article 122 ter, when formulated by the General Council of the Judiciary."

Four. A new article 122 ter is hereby introduced, which shall read as follows:

"Article 122b. *Procedure for judicial authorization of conformity of a decision of the European Commission on international data transfer.*

1. The procedure for obtaining the judicial authorization referred to in the fifth additional provision of the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights, will begin with the request of the data protection authority addressed to the competent Court to rule on the conformity of a decision of the European Commission on the international transfer of data with the law of the European Union. The request shall be accompanied by a copy of the file pending before the data protection authority.

2. In addition to the data protection authority, the parties to the proceedings shall be those who were parties to the proceedings before it and, in any case, the European Commission.

3. The resolution of admission or inadmissibility of the proceeding will confirm, modify or lift the suspension of the proceeding for possible violation of data protection regulations before the data protection authority, from which this judicial authorization proceeding originates.

4. Once the application has been admitted for processing, the competent Court shall notify the data protection authority so that it may notify those involved in the proceedings before it so that they may appear within a period of three days. Likewise, the European Commission shall be notified to the same effect.

5. At the end of the period mentioned in the preceding paragraph, the request for authorization shall be forwarded to the parties so that within a period of ten days they may present their arguments as they deem appropriate, at which time they may request the taking of any evidence they deem necessary.

6. At the end of the evidentiary period, if either party has so requested and the court deems it appropriate, a hearing shall be held. The Court may decide the scope of the issues on which the parties shall focus their arguments at such hearing.

7. Once the procedures mentioned in the three preceding paragraphs have been completed, the competent Court shall adopt one of these decisions within ten days:

a) If it considers that the European Commission's decision is in accordance with European Union law, it will issue a judgment declaring this to be the case and refusing the authorization requested.

b) If it considers that the decision is contrary to European Union law, it shall issue an order referring the validity of the decision to the Court of Justice of the European Union for a preliminary ruling under the terms of Article 267 of the Treaty on the Functioning of the European Union.

Authorization may only be granted if the European Commission decision in question is declared invalid by the Court of Justice of the European Union.

8. The regime of appeals shall be as provided in this ley."

Seventh final provision: *Modification of Law 1/2000, of January 7, 2000, on Civil Procedure.*

Article 15 bis of Law 1/2000, of January 7, of Civil Procedure is amended and shall read as follows:

"Article 15 bis. *Intervention in antitrust and data protection proceedings.*

1. The European Commission, the National Commission for Markets and Competition and the competent bodies of the autonomous communities within the scope of their competences may intervene in antitrust and data protection proceedings, without having the status of a party, on their own initiative or at the request of the judicial body, by providing information or submitting written observations on matters relating to the application of articles 101 and 102 of the Treaty on the Functioning of the European Union or articles 1 and 2 of Law 15/2007, of July 3, 2007, on the Defense of Competition. With the permission of the corresponding judicial body, they may also submit oral observations. For these purposes, they may request the competent court to send or have sent to them all the documents necessary for an assessment of the case in question.

The provision of information shall not include data or documents obtained within the scope of the circumstances of application of the exemption or reduction of the amount of the fines provided for in Articles 65 and 66 of Law 15/2007, of July 3, 2007, on the Defense of Competition.

2. The European Commission, the National Commission for Markets and Competition and the competent bodies of the autonomous communities shall provide the information or submit the observations provided for in number ten above.

days before the trial proceedings referred to in Article 433 or within the time limit for opposition or contestation of the appeal filed.

3. The procedural provisions of the preceding paragraphs shall also apply when the European Commission, the Spanish Data Protection Agency and the autonomous data protection authorities, within the scope of their competences, consider it necessary to intervene in a process affecting matters relating to the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016."

Eighth final provision. *Modification of the Organic Law 6/2001, of December 21, 2001, on Universities.*

A new letter l) is included in section 2 of article 46 of Organic Law 6/2001, of December 21, 2001, on Universities, with the following content:

"(\) Training in the use and security of digital media and in the assurance of fundamental rights on the Internet."

Ninth final provision. *Modification of Law 41/2002, of November 14, 2002, basic law regulating patient autonomy and rights and obligations regarding clinical information and documentation.*

Section 3 of article 16 of Law 41/2002, of November 14, 2002, which regulates patient autonomy and the rights and obligations regarding clinical information and documentation, is amended to read as follows:

"Article 16.

3. Access to the clinical history for judicial, epidemiological, public health, research or teaching purposes is governed by the provisions of current legislation on the protection of personal data, and by Law 14/1986, of April 25, 1986, General Health Law, and other applicable regulations in each case. Access to the clinical history for these purposes requires the preservation of the patient's personal identification data, separated from those of a clinical-healthcare nature, so that, as a general rule, anonymity is assured, unless the patient himself has given his consent not to separate them.

The cases of investigation provided for in section 2 of the seventeenth additional provision of the Organic Law on Personal Data Protection and Guarantee of Digital Rights are excepted.

An exception is made for cases of investigation by the judicial authority in which it is considered essential to unify the identification data with the clinical-health care data, in which case the provisions of the judges and courts in the corresponding process shall apply. Access to clinical history data and documents is strictly limited to the specific purposes of each case.

When necessary for the prevention of a serious risk or danger to the health of the population, the health administrations referred to in Law 33/2011, of October 4, 2011, General Law on Public Health, may access patient identification data for epidemiological reasons or for the protection of public health. The access will have to be carried out, in any case, by a health professional subject to professional secrecy or by another person subject, likewise, to an equivalent obligation of secrecy, prior motivation by the Administration requesting access to the data."

Tenth Final Provision: *Modification of the Organic Law 2/2006, of May 3, 2006, on Education.*

A new letter l) is included in section 1 of article 2 of Organic Law 2/2006, of May 3, 2006, on Education, which shall read as follows:

> *"l)* Training to ensure the full insertion of students in the digital society and the learning of a safe use of digital media and respectful of human dignity, constitutional values, fundamental rights and, particularly, with respect and guarantee of individual and collective privacy."

Eleventh final provision. *Modification of Law 19/2013, of December 9, on transparency, access to public information and good governance.*

Law 19/2013, of December 9, 2013, on transparency, access to public information and good governance, is amended as follows:

A new article 6 bis is added, with the following wording:

"Article 6 bis. *Registration of treatment activities.*

The subjects listed in Article 77.1 of the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights shall publish their inventory of processing activities in application of Article 31 of the aforementioned Organic Law."

Two. Paragraph 1 of Article 15 shall read as follows:

"If the information requested contains personal data revealing ideology, trade union affiliation, religion or beliefs, access may only be authorized with the express written consent of the data subject, unless the data subject had manifestly made the data public prior to the request for access.

If the information includes personal data referring to racial origin, health or sex life, includes genetic or biometric data or contains data relating to the commission of criminal or administrative offenses that do not entail a public warning to the offender, access may only be authorized with the express consent of the person concerned or if it is covered by a regulation with the rank of law".

Twelfth final provision. *Modification of Law 39/2015, of October 1, of the Common Administrative Procedure of Public Administrations.*

Sections 2 and 3 of Article 28 of Law 39/2015, of October 1, of the Common Administrative Procedure of Public Administrations, are amended to read as follows:

"Article 28.

2. The interested parties have the right not to provide documents that are already in the possession of the acting administration or have been prepared by any other administration. The acting administration may consult or request such documents unless the interested party objects. Opposition will not be possible when the provision of the document is required within the framework of the exercise of sanctioning or inspection powers.

The Public Administrations shall collect the documents electronically through their corporate networks or by consulting the data intermediation platforms or other electronic systems enabled for this purpose.

In the case of mandatory reports already prepared by an administrative body other than the one processing the procedure, these must be sent within ten days of their request. Once this period has expired, the interested party shall be informed that he/she may provide this report or wait for it to be sent by the competent body.

3. The Administrations will not require the presentation of original documents from the interested parties, unless, exceptionally, the applicable regulations establish otherwise.

Likewise, the Public Administrations will not require data or documents from the interested parties that are not required by the applicable regulations or that have been previously submitted by the interested party to any Administration. For these purposes, the interested party must indicate at what time and before which administrative body he/she submitted the aforementioned documents, and the Public Administrations must collect them electronically through their corporate networks or by consulting the data intermediation platforms or other electronic systems enabled for this purpose, unless the express opposition of the interested party is recorded in the procedure or the applicable special law requires his/her express consent. Exceptionally, if the Public Administrations are unable to obtain the aforementioned documents, they may request the interested party to provide them again."

Thirteenth final provision: *Amendment of the revised text of the Workers' Statute Law.*

A new article 20 bis is added to the revised text of the Workers' Statute Law, approved by Royal Legislative Decree 2/2015, of October 23, with the following content:

"Article 20 bis. *Workers' rights to privacy in relation to the digital environment and to disconnection.*

Workers have the right to privacy in the use of digital devices made available to them by the employer, to digital disconnection and to privacy from the use of video surveillance and geolocation devices under the terms established in current legislation on the protection of personal data and guarantee of digital rights."

Fourteenth final provision: *Modification of the revised text of the Basic Statute of the Public Employee Law.*

A new letter j bis) is added to Article 14 of the consolidated text of the Basic Statute of the Public Employee Law, approved by Royal Legislative Decree 5/2015, of October 30, which shall be worded as follows:

"(ja) To privacy in the use of digital devices made available to them and against the use of video surveillance and geolocation devices, as well as to digital disconnection under the terms established in the current legislation on the protection of personal data and guarantee of digital rights."

Fifteenth final provision. *Regulatory development.*

The Government is empowered to develop the provisions of Articles 3.2, 38.6, 45.2, 63.3, 96.3 and the sixth additional provision, under the terms established therein.

Sixteenth Final Provision. *Entry into force.*

This Organic Law shall enter into force on the day following its publication in the Official State Gazette.

Therefore,
I command all Spaniards, individuals and authorities, to keep and enforce the observance of this organic law.

Madrid, December 5, 2018.

FELIPE R.

The President of the Government,
PEDRO SÁNCHEZ PÉREZ-CASTEJÓN

code: BO-EA- 201-8 16673
Verifiable at http ://www.boe.es