



GENERAL DATA
PROTECTION
REGULATION REPORT

2016

ECIJA

Report -General Data Protection Regulation

BACKGROUND

P.4

MAIN DEVELOPMENTS

P.7

MEASURES AND TERMS

P.12

ECIJA SOLUTIONS

P.15

FAQS

P.16

Privacy
and Data
Protection
Department

www.ecija.com



Report -General Data Protection Regulation

The approval, on 14 April 2016, of the General Data Protection Regulation ends with the path undertaken years ago to homogenize the different regulations on personal data in the European Union, unifying legislation in all Member States. A milestone that means for companies the challenge of adapting to the obligations and requirements set by the European regulation and a competitive opportunity to operate in the global market.

It is therefore essential for all organizations (companies and institutions, among others) processing personal data to take into account the new applicable rules in the protection of the rights of citizens, as well as the competitive opportunities that this new regulation offers to compete in a global market.

Thus, the knowledge of these rules becomes a fundamental basis for organizations, providing legal certainty for their operations, providing value to customers and users with respect to their rights and privacy, reducing punitive and reputational risks and optimizing their resources and processes in relation to the processing of personal data.

The Privacy and Data Protection Department of ECIJA has prepared this Report in order to analyze the developments that the Regulation involves for companies and individuals in their daily activities, facilitating their adaptation to the new rules, promoting the culture of compliance and respect for privacy and protection of individuals.

Privacy and Data Protection
Department ECIJA



Leading Firm in advising in Technology, Media and
Telecommunications

01. BACKGROUND

The right to data protection is configured as a fundamental right of individuals, as stated in the different national constitutions. A right that has its origin in the Convention No. 108 and that was consolidated with the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.

The unstoppable advances of technology, along with the requirements set by the events themselves, have revealed again and again the need to advance in a unified regulation of the right to data protection. A Digital Single Market highlights the need to adopt rules that ensure the protection of individuals and that enable the advance of new business models based on the possibilities provided by the new technologies.

Thus, at the beginning of 2012, the General Data Protection Regulation began a long journey until

its approval. A regulation that aims to recognize the majority of the companies and institutions in the processing of personal data, providing Europe with a pioneering regulation in accordance with the XXI Century.

Certain formal obligations, such as the registration of files recognized by the Directive, give way to the adoption of guarantees and safeguards by the data controllers, from the conception of privacy as a value in the design of products.

A conciliation of the protection of the right of individuals and the development of digital economy, oriented to the recognition of the autonomy of the individuals to decide about their personal data, is addressed under the new rules, where transparency comes first. A rule of the present prepared for the society of the future.

02. MAIN DEVELOPMENTS

The approval of the European Data Protection Regulation means the incorporation to our legal system of new legal issues that, without any doubt, shall affect directly to companies, consumers and users. In particular, the main objective of this regulation is to provide a higher control to the individuals affected in relation to their private information and thus, to adapt the European regulation, to a greater extent, to the information society. A necessary harmonization at a European level of the demands and requirements regarding data protection.

Main developments for the companies:



Principle of **RESPONSIBILITY**: Companies shall implement measures that enable them to prove that they are adopting all the necessary measures to develop a correct data processing.



Obligation, in certain cases, to perform **IMPACT ASSESSMENTS** that determine the specific risks that involve the processing of certain personal data.



Progress in the adoption of data protection principles by **DEFAULT AND FROM THE DESIGN** aimed to adopt the culture of privacy within the company and to ensure the privacy of individuals.



Possibility for the data controller to charge a **FEE**, taking into account the administrative costs of answering the requests of the right of access by the individuals.



Designation of a Data Protection Officer (**DPO**).



Communication of **PERSONAL DATA BREACHES** to the supervisory authority and to the data subjects, as soon as the breach is known and not later than 72 hours after having become aware of it.



ONE-STOP-SHOP. Companies shall have as a partner a single supervisory authority. It is estimated that this measure will save 2,3 billion euros per year.



Specific rules that will facilitate **INNOVATION**. The rules shall establish that the data protection guarantees are incorporated in the products and services since its first phases of development.

Main developments for the companies



Progress in the adoption of **GUARANTEES** on the processing of personal data as well as the individuals and companies involved in them. In this sense, the selection of data processors that provide guarantees to such data processing will play an important role.



Principle of **TRANSPARENCY** in the processing of personal data and principle of **ACCOUNTABILITY**. Simplification of the legal notices and clauses, facilitating its understanding by the data subjects.



Elimination of the current obligation of **REGISTRATION** of the files in the Agencies and Data Protection Authorities, replacing this obligation by an internal control, inventory of the files, data processed and flows of the processing performed by the companies.



"A rule of the present prepared for the society of the future".

Main developments for particulars:



Greater **TRANSPARENCY** and **INFORMATION** to citizens by the organizations which process their personal data, facilitating further information on data conservation periods, the purpose of the processing and the companies who will participate in it.



Consolidation of the **RIGHT TO BE FORGOTTEN**. The data subjects may revoke the consent given for the processing of their personal data at any time, being able to require the removal and elimination of the convenient data from social networks and Internet search engines. In the same way, the protection of minors is reinforced in this matter.

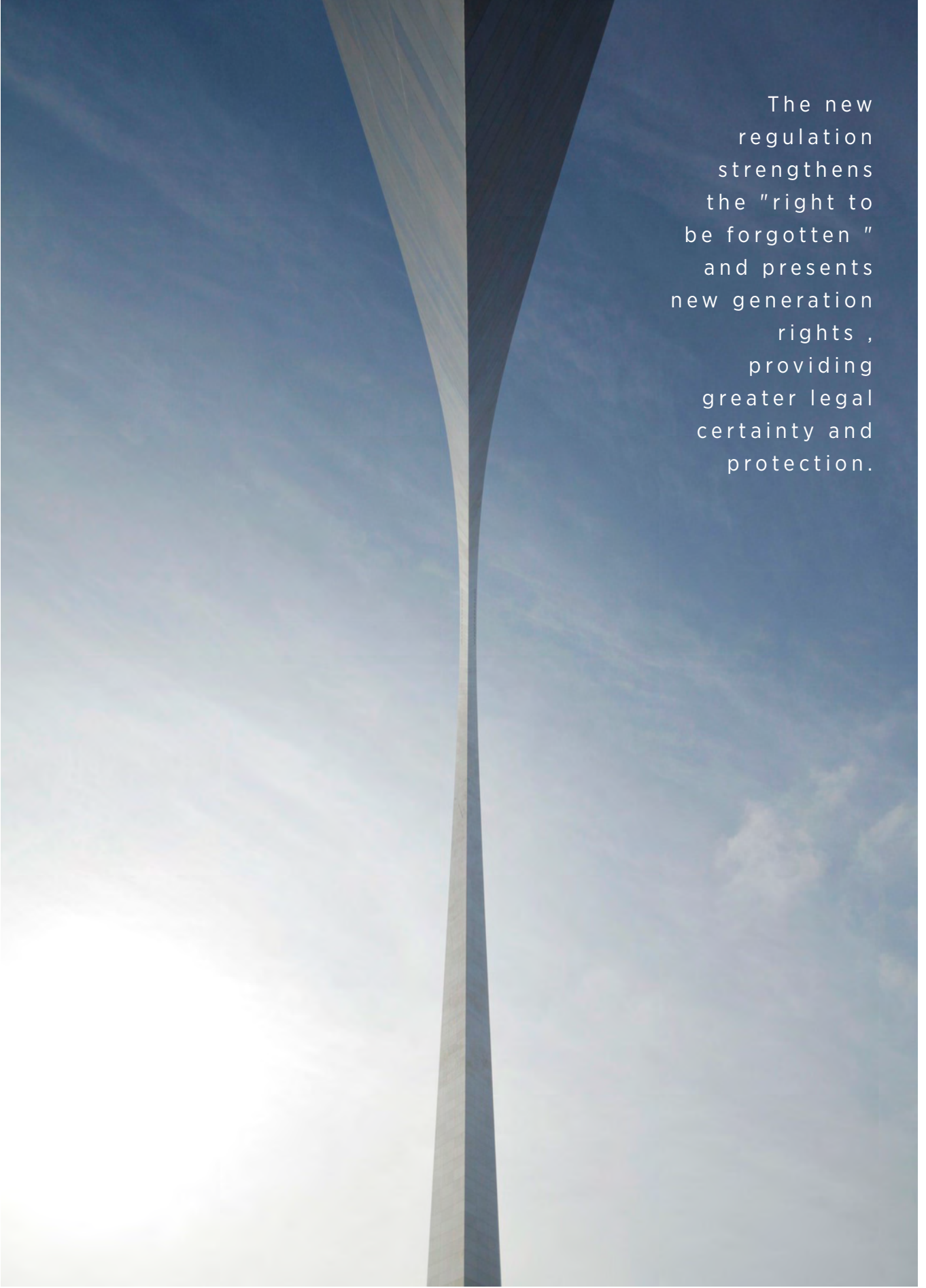


Right to **DATA PORTABILITY**. It will be allowed to transfer the personal data in an easier way from an Internet service provider to another, always giving control to citizens to decide on its final processing.

Transparency and
information

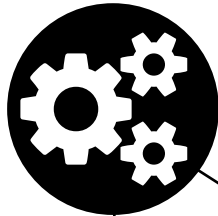
Right to be forgotten
and protection of
minors

Data Portability



The new
regulation
strengthens
the "right to
be forgotten "
and presents
new generation
rights ,
providing
greater legal
certainty and
protection.

Other developments to take into account:



Type of data:

Expansion of the data considered sensitive, including genetic and biometric data.

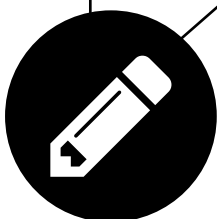
Guarantees:

Establishing more strict guarantees and monitoring mechanisms regarding international data transfers out of the European Union.



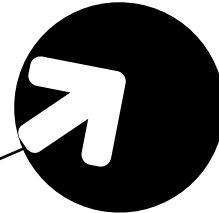
Seal of compliance:

Establishing seals of compliance (European Data Protection Seal).



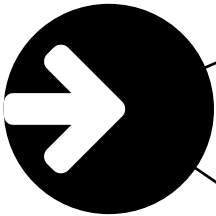
Complaints:

Possibility to lodge complaints through users associations and recognition of the possibility to demand compensation for the damages derived for the unlawful processing of personal data.



Penalties:

The quantities of the penalties associated to the breach of the legal provisions may reach 20 million euros or 4% of the total worldwide annual turnover.





REGISTRATION

DPO

CONSENT

RESPONSABILITY

IMPACT ASSESSMENTS

SECURITY

03. MEASURES AND TERMS:

The General Data Protection Regulation establishes a transitional period of two years since its entry into force, that is, 20 days since its publication in the Official Journal of the European Union.

The provisions contained in the Regulation are directly applicable to all Member States.



Which are
the main
developments
for the
companies?

1. Registration

An internal and written registration must be carried out keeping record of the different activities developed in the company that involve data processing, since the obligation to register the files of the company in the Register of the Spanish Data Protection Agency was eliminated.

2. DPO

A Data Protection Officer shall be designated provided that:

- The processing is carried out by a public authority.
- The main activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale.
- The main activities consist of processing on a large scale of special categories of data.

3. Consent

The consent to process personal data must be unequivocal, free and revocable, as well as being given by a clear affirmative act.

4. Responsibility

Responsibility of those carrying out the data processing in order to demonstrate that the requirements under the Regulation are met. This is a proactive responsibility, ie, it must be demonstrated that the company has materialized these requirements through, for example, policies, procedures, controls, etc.

5. Impact assessments

Before performing certain processing (profiling, processing on a large scale of special categories of data, inter alia) companies shall develop an impact assessment, in which the possible risks that the new data processing may involve are analyzed.

6. Privacy by design / by default

Data protection by design and by default: companies that process personal data must take into account all the provisions of the regulations that may affect them before performing the processing, for example, before developing a computer tool, they shall apply the corresponding technical and organizational measures. Likewise, they should limit the process to indispensable data as to perform certain processing, ensuring that, by default, only those data necessary for the specific purposes of the processing shall be processed.



Which are
the main
developments
for the
companies?



04. ECIJA SOLUTIONS

How can ECIJA help you?

ECIJA offers specialized legal advice based on a thorough understanding of the regulations and requirements of the different business models and sectors, facilitating the approach to the legal provisions and their application taking into account the business idiosyncrasy, from the conciliation between technology and law.

During the adaptation process derived from the new European regulation, ECIJA offers, among others, the following services:

- Adoption of procedures or redefinition of corporate policies.
- Advice for the performing of impact assessments / risks and implementation of privacy by design or by default privacy processes.
- Training for employees about the compliance with the new regulation.
- Development of compliance audits.
- Development and definition of risk maps according to the business sector.
- Advice in the definition of functions of the Data Protection Officer.

In addition, together with the professional team of the Company, ECIJA owns different tools for the management of the data protection regulation, which facilitate functionalities adapted to the requirements of the European Data Protection Regulation. A legal compliance solution to improve the management efficiency and to facilitate the accountability principle (demonstration of compliance).

05. FAQs

Q: When will the General Data Protection Regulation enter into force?

The entry into force of the Regulation will take place 20 days after its publication in the Official Journal of the European Union. However, its legal provisions will only apply 2 years after its publication in the Official Journal of the European Union.

Q: What will be the scope of application of the new Regulation?

The scope of the Regulation involves the data processing carried out within the framework of the activity of data controllers established in the EU.

Q: Is the regime of the duty of information and consent modified?

Yes. The data controller shall provide the data subject any complementary information that is necessary to ensure fair and transparent processing of data, taking into account the circumstances in which the processing is performed and the origin of the data.

Q: What developments are introduced by the new configuration of the “right to be forgotten”?

In particular, the Regulation recognizes the right for data subjects to have their personal data deleted and no longer processed if such data are no longer necessary for the purposes for which they were collected or processed, if the data subjects have withdrawn their consent for the processing, or they freely oppose to that processing.

The new regulation
will entry into force
next 2018

Q: What penalties will be imposed to the companies for breaching the new Data Protection Regulation?

The penalties will be increased with respect to those established in the Spanish Data Protection Law.

a) Financial penalties up to 10,000,000 euros or up to 10% of the total worldwide annual turnover of the preceding financial year.

b) Financial penalties up to 20,000,000 euros of the total worldwide annual turnover.

Q: What shall the companies take into account in regards to personal data protection?

The new Regulation incorporates the obligation for companies to act according to the “accountability principle”. This involves the performing of regular impact assessments, as long as the data processing involves a risk for the rights and liberties of the data subjects and the adoption, before and during the processing, of the concrete technical and organizational measures to determine the risks that certain data processing may involve.



Q: Is it compulsory to designate a Data Protection Officer?

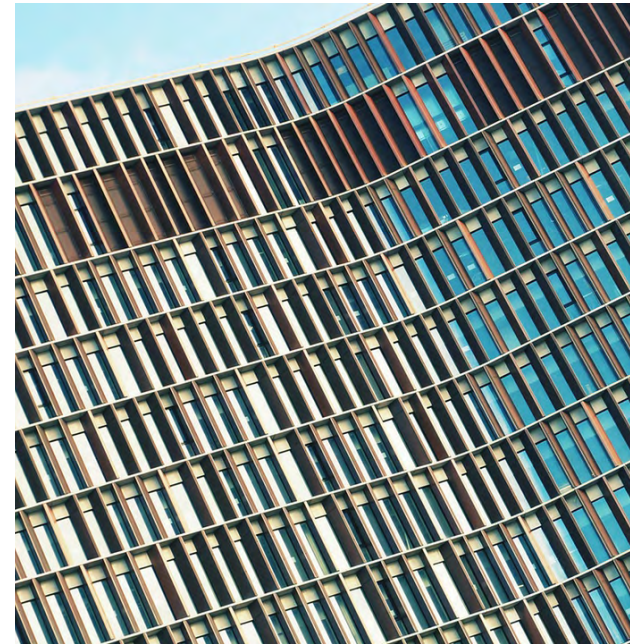
The companies and organizations shall be obliged to designate a DPO (either internally or outsourced to a third party) when the main activities of the data controller consist of processing on a large scale of special categories of data or that require regular and systematic monitoring.

Q: Shall companies and organizations continue registering files in the Spanish Data Protection Agency?

No. The Regulation focuses the registration obligations from an internal point of view with respect to the organizational environment of companies and organizations. They shall complete registration forms of processing internally and in writing, whose content shall be very similar to the current Electronic Notification System of the Spanish Data Protection Agency (NOTA System). This internal registration shall be available when required by the Spanish Data Protection Agency, who will be enabled to get it within the exercise of its powers of inspection.

Q: What national authority will be competent to handle the questions derived from the action of a company or organization that acts in more than one Member State of the EU?

The “one-stop-shop” principle will be applicable. Thus, in certain cases, the Control Authority of the place where it is located the principal place of business of a data controller or processor in the European Union acts as the main control authority for the cross-border data processing.



Q: Shall the companies and organizations notify the personal data breaches or the information leakages to the Spanish Data Protection Agency or to the data subjects?

Yes. In case that there is a data breach that may damage the rights of the data subjects, the data Controller shall notify it to the Spanish Data Protection Agency in seventy two (72) hours, and notify it to the data subjects as soon as possible. The communication shall describe the nature of the personal data breach and the recommendations for the data subject to reduce the risks.

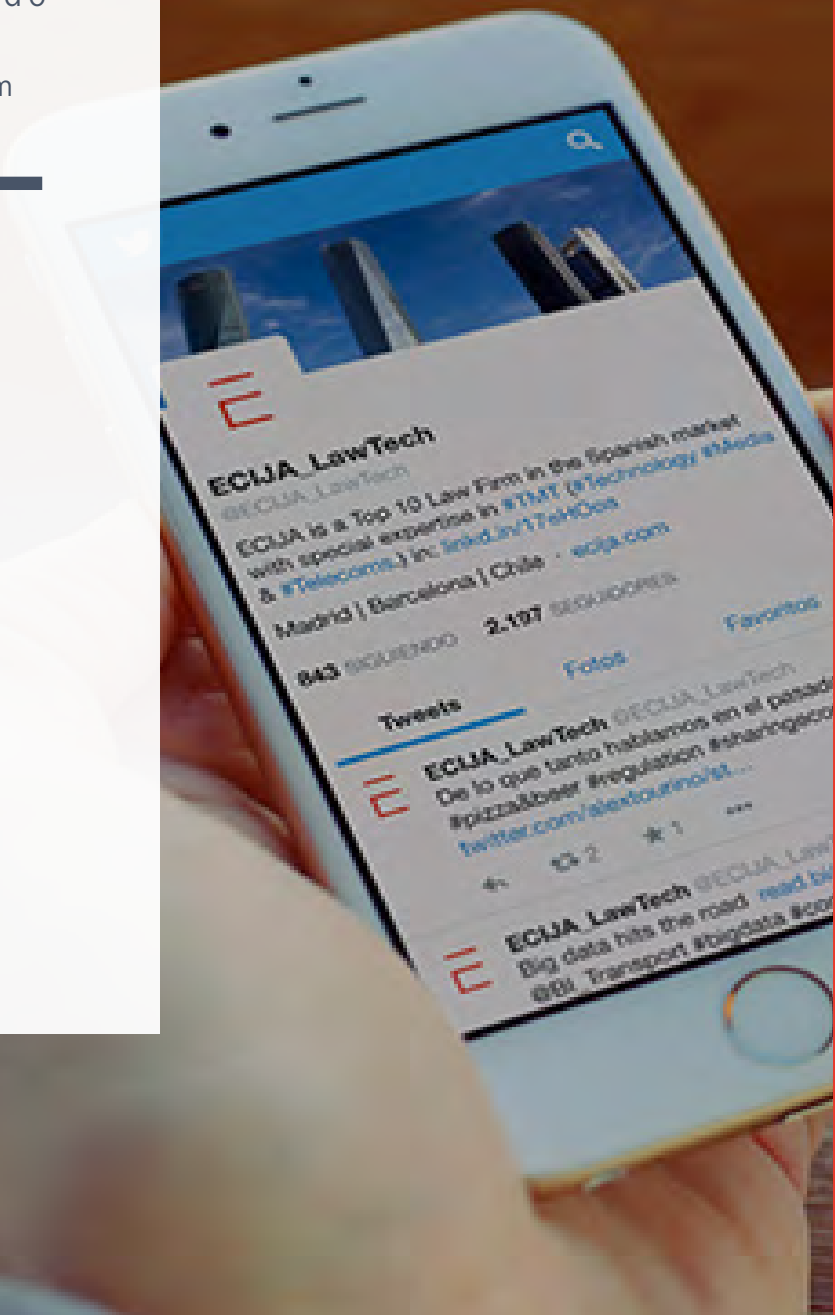
Q: How should the companies and organizations proceed until the moment when the provisions of the new Data Protection Regulation are applicable?

The Regulation imposes large obligations that may require significant organizational, technical, economic and human efforts. Thus, a complete implementation of the obligations of the Regulation necessary implies that the organizations become familiar with the content of the Regulation and start designing the plans for its implementation from the very moment of its approval.

Contact

Alonso Hurtado
Partner
alhurtado@ecija.com
91.781.61.60

Carlos Pérez
Partner
cperez@ecija.com
93.380.82.55





www.ecija.com