# IMPLEMENTING THE EUROPEAN REGULATION ON DATA PROTECTION (GDPR)

MARIMÓN

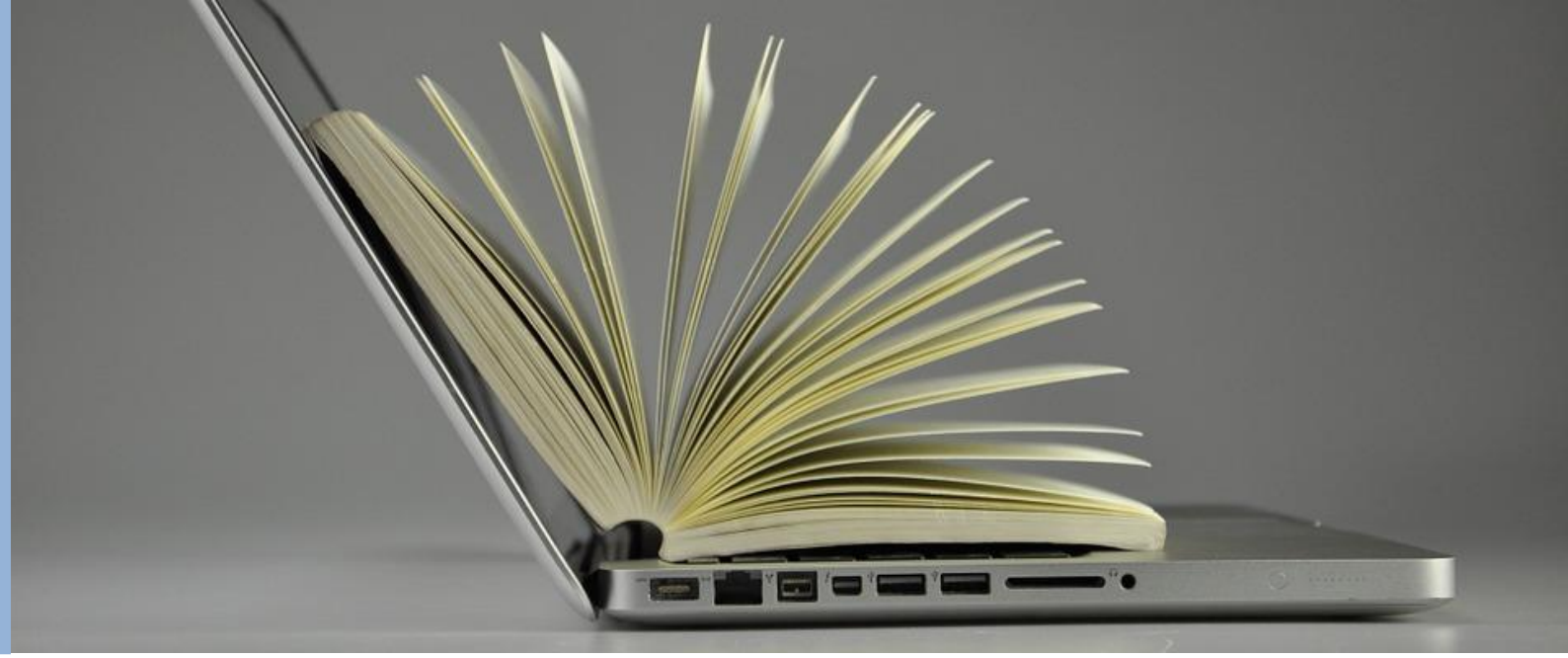
ABOGADOS

The new 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 personal data and on the free movement of such data ("GDPR"), came into force on 25 May 2016 and will be fully implemented on 25 May 2018.

Recently the draft of the reform of the Organic Law on Data Protection was presented before the Council of Ministers with the purpose of adapting the national regulations to the new European framework. This draft includes particular updates such as the reduction of the age at which minors may consent to the processing of their data to 13 years, and the regulation on the processing of data of deceased persons, among others.

The new Regulation seeks to reinforce the responsibility of organizations that should guarantee compliance with requirements concerning the protection of data and be capable of proving their compliance by documenting their processing of this data. The companies currently have a timeframe of less than a year to carry out all the necessary actions to adopt the new legal framework.

The companies will have to carry out a series of changes before 25 May 2018 in order to comply with the new Regulation.



## MAIN ACTIONS TO CARRY OUT:

**PHASE 1.-** Appoint a Data Protection Officer (DPO)

**PHASE 2.-** Record processing activities

**PHASE 3.-** Analyze risks

**PHASE 4.-** Carry out impact assessment

**PHASE 5.-** Review internal procedures

**PHASE 6.-** Adapt the existing documentation

**PHASE 7.-** Document compliance

## **PHASE 1.-** APPOINT A DATA PROTECTION OFFICER

In order to manage and coordinate personal data of the organization in the correct way, it may be necessary in some cases to appoint the position of the Data Protection Officer (DPO). The DPO will be responsible for the information, supervision of compliance with the Regulation, and advice and cooperation regarding the fulfillment of the data protection Regulation. It is worth remembering that the incorporation of a DPO before May 2018 can be a significant initial advantage for the organization.

It is compulsory for the organizations to appoint a DPO if they fall under the following categories:

- Public organizations;
- Entities which require routine and systematic monitoring of personal data on a large scale;
- Entities whose main activity consists of the processing of special categories of data;
- When required by a EU member nation or by the European Union.

In certain cases, even when the organization is not formally obliged to define this position, it is recommended that companies of a certain size appoint a DPO for the sake of strengthening their compliance with the Regulation on data protection and to minimize the handling risks. It is also common that groups of companies share unified criteria for all their subsidiaries regardless of their size.

According to the draft of the Spanish law, the following, among others, could be considered to fall into these criteria:

- Insurance and reinsurance companies.
- Distributors and marketers of electrical energy or natural gas.
- Entities responsible for credit information systems.
- Entities that carry out advertising activities which include an analysis of preferences or creation of profiles.
- Health facilities.
- Educational institutions that offer formal education, universities.
- Professional bodies.
- Online gambling companies.

## **PHASE 2.-** RECORD PROCESSING ACTIVITIES

To effectively measure the impact of the European Regulation on data protection within companies, they must first define in detail their flows of data and the processing they carry out.

The implementation of the GDPR entails the obligation to record the processing activities. For this, companies must keep an internal log with detailed information on their data processing and their level of compliance with the Regulation. This information must be made available to the Supervisory Authority as and when required.

Therefore, before May 2018, companies –whether responsible for or charged with the processing– must prepare this internal log in order to identify and define the data processing carried out within the organization. In addition to compliance with the Regulation, this will allow for an effective control of the personal data being processed, as well as an easier detection of the possible risks which exist during such processing.

## **PHASE 3.-** ANALYZE RISKS

Once the processing activities have been recorded, organizations must identify the procedures which they must carry out to prevent or otherwise minimize the detected risks, with the aim of adapting to the current and future requirements concerning the protection of data. Among the procedures due to be carried out they must prioritize those relating to the processing of data that pose the greatest risks to the rights and liberties of the persons in question.

This prioritization must be enforced rigorously and criteria must be established according to the sensitivity of the data, the environment in which the processing is carried out and the volume of the data being processed.

During the analysis of the risks, in order to prevent or otherwise minimize the risks, where appropriate, certain technical and organizational security measures must be adopted in order to prevent the loss of information, the unintentional destruction of data or the access of unauthorized third parties, and also to guarantee integrity, availability and the unchangeability of the data processed.

## PHASE 4.- ASSESS THE IMPACT

In the event of detecting that some personal data processing carried out poses a severe risk to the rights and liberties of the parties concerned, a **data-protection impact assessment** must be carried out (PIA in English) for each one of the processes.

**When must the Impact Assessment (PIA) be carried out?**

- Prior to any processing of data which could seriously infringe the rights and liberties of the individuals.

**In what cases must an Impact Assessment (PIA) be performed?**

- When processing operations include a "*systematic and extensive assessment of personal aspects relating to natural persons*¨;
- For large-scale processing of sensitive data;
- For large scale systematic surveillance of a public area.

Even then, in certain cases where there is no need to carry out the Impact Assessment, it is recommended that it be carried out nonetheless, given that it is a useful tool for the person in charge to have greater control over the relevant data processing.

The Impact Assessment is an essential measure to ensure accountability. It not only facilitates the fulfillment of the Regulation, but it also provides evidence of compliance with the Regulation.

The final result of an Impact Assessment is a report which compiles the characteristics of the evaluated processing and the decisions taken to prevent and minimize the risks, starting with the identification, analysis, evaluation and processing (management of risks) once the issues such as the legitimate interest (where appropriate) or the need and the proportionality of the processing operations have been analyzed.

## PHASE 5.- REVIEW INTERNAL PROCEDURES


To guarantee a high level of protection of personal data, organizations must implement internal procedures which ensure the protection of data at all times, taking into consideration the entirety of the unforeseen situations which can affect the processing of personal data (e.g. security failure, management of requests for correction or for access, change of service provider, among others).

**Organization of the procedures entails:**

- Taking into consideration the protection of personal data from the design;
- Informing and organizing personnel;
- Addressing the claims and requests of the parties concerned with regards to the processing of their personal data;
- Establishing a series of steps for the correct handling of security breaches which must be informed to the relevant Supervisory Authority and, in certain cases, the affected parties too, within 72 hours.

## PHASE 6.- ADAPT THE EXISTING DOCUMENTATION

**a) How to gather consent in each of the data processing proceedings:**

Companies must review the consent given beforehand and verify that it complies with the new demands of the GDPR. In particular, only consent given by a declaration or clearly affirmative action will be valid. If this is not the case, the consent will not be considered valid and the company will have to opt to:

- Abstain from processing such data and proceed to erase it, or
- Gather once again the consent of the affected parties through means which conform to the GDPR.

For the consent to be considered valid and in order for it to still be used, it must be given by the party concerned through the expression of their free, specific, informed and unmistaken wish in a statement or clearly affirmative action.

Consent collected as a result of mere silence or inactivity of the party concerned will not be valid and must be gathered once again.


**b) Reviewing the informative clauses and establishing additional informative measures:**

The requirements regarding the obligation to inform the persons concerned have increased with the addition of further requirements. This means that the clauses must contain the following additional aspects:

- contact details of the Data Protection Officer, where appropriate;
- the legal basis or entitlement of the processing;
- the term and criteria for keeping the information.

- outlook for international transfers;
- the right to file a claim before the Supervisory Authorities;
- the possibility for the persons concerned to exercise their rights (of access, rectification, elimination, processing restriction, data portability, opposition, and not to be the object of individual automated decisions); and
- existence of automated decisions or creation of profiles.

The procedures, templates or forms existing in companies and put together in accordance with the LOPD must be reviewed and adapted before the GDPR is fully implemented.

**c) Contracts between data controllers and data processors:**

The organization will have to review the pre-existing contracts commissioning data processing whereby third parties may access the company's personal data, changing some clauses as follows:

- Security measures: carry out a prior risk assessment and determine the security measures to be applied with regards to the processing.
- Rights of the interested individual/s: these have increased in comparison to the traditional ARCO rights.
- Notification of any security violation: foresee a procedure of notification of any security violations.

## PHASE 7.- DOCUMENT COMPLIANCE

To verify compliance with the GDPR, the organization must make available all the necessary documentation. The actions taken and the documents drafted in each step must be reviewed and updated regularly to ensure the fulfillment of the data protection Regulation. As a result, the company must put together a document file, either physical or electronic, which proves that the processing of personal data that it carries out is done in compliance with the Regulation and that the relevant technical and organizational measures are applied.

**The file must contain the following elements at the very least:**

Documentation concerning the processing of personal data carried out:

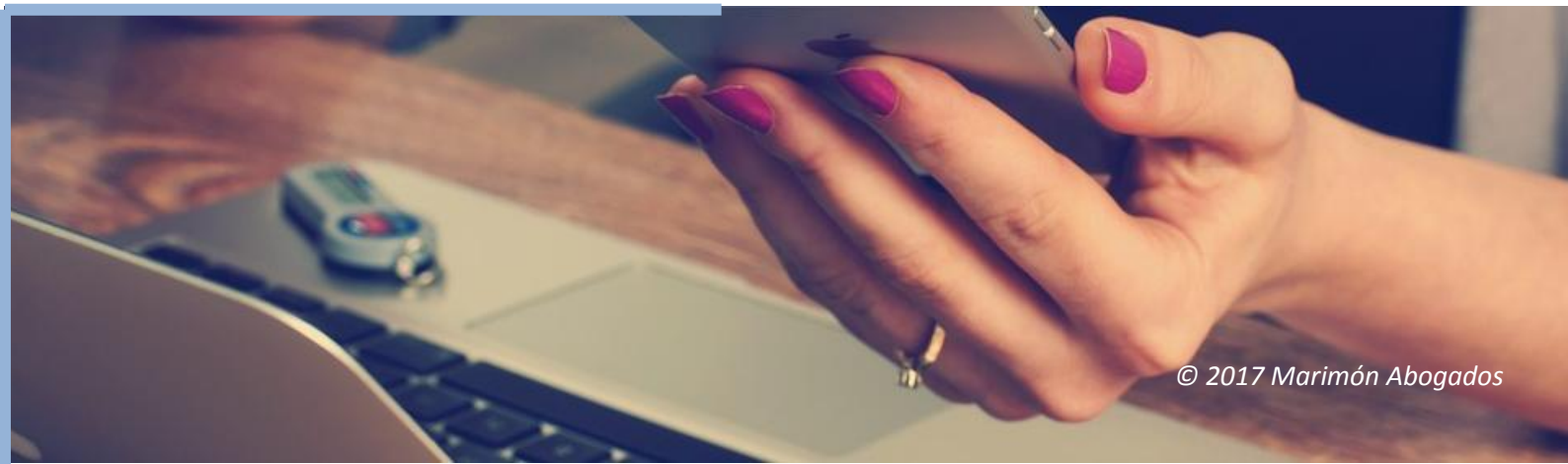
- Record of the processing activity.
- Data-protection impact assessment.
- The necessary documentation which sets up international transfers of data.

Personal data:

- Documents with information on the party concerned.
- Consent forms of the parties concerned.
- Procedures put in place for the exercise of persons´ rights.

Various contracts and agreements:

- Contracts with the processing officers.
- Internal procedures regarding security breaches.
- Evidence that the parties concerned gave their consent prior to the processing of their personal data.




## LUIS MARIMÓN

lmarimon@marimon-abogados.com


Partner at Marimón Abogados. He works at the department of Corporate Law and is Head of the area of IT/IP.


## EDUARD BLASI

blasi@marimon-abogados.com


Senior lawyer at Marimón Abogados. He works at the department of IT/IP and is a Data protection expert.


**Barcelona**
Paseo de Gracia, 118
08008 Barcelona.
Tel.:+34 93 415 75 75
Fax:+34 93 415 83 11

**Madrid**
Paseo de Recoletos, 16
28001 Madrid.
Tel.: +34 91 310 04 56
Fax: +34 91 702 36 36

**Seville**
Balbino Marrón, 3
Planta 5ª-17 (Edificio Viapol)
41018 Sevilla.
Tel.: +34 954 657 896