Everything you have to know about General Data Protection Regulation

On May 25th 2016 the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND COUNCIL of April 27th 2016 on the protection of natural persons with regard to the processing of personal data and on the free transfer of such data (General Data Protection Regulation – hereinafter GDPR) came into force, whose application will not become effective until May 25th 2018. Since Spanish Personal Data Protection Draft Act to adapt national provisions to the new European framework is still in progress, these last months are of crucial importance; that's why companies have gone through an adaptation period and progressive alignment to the GDPR.

Hereunder we explain the main steps and/or the modifications that companies treating personal data should carry out to comply with the GDPR.

1. Review and adapt the existing documentation:

a. Changes in the consent of data for processing any data:

The GDPR does not allow treating personal data on the basis of tacit consent. It will be mandatory to have a statement of the concerned subject expressing his accordance and willingness with treating his personal data. Therefore, businesses have to review the consent forms previously received and verify if they comply with the new requirements of the GDPR: otherwise, they will have to obtain express consent if it lacks.

b. Changes in information right:

In case of collecting personal data, until now, it was mandatory to inform in which file they were going to be added, the identity of the treatment officer, the purpose of data collection and if there were data transfer or rights data transfer (ARCO rights). The new GDPR increases the duty to report to the concerned people, requiring the following mandatory information:

- Processing data legal base.
- The contact details of the Data Protection Officer (if existing).
- The period and criteria of the data retention.
- The estimate of international transfers.
- The authority control (the Spanish Data Protection Agency).
- Automatic treatment or profiling.
- The rights of the concerned subjects and their modality of exercise (rights to access, rectify, erase data, to restrict processing, right to oblivion, right to data portability).

Therefore, all companies will have to review their consent forms (online and offline versions) and modify them according to the requirements above indicated before the GDPR comes into force.

c. Data processing contracts:

Data processing contracts with third parties (managers, external computer managers, Marketing companies, etc.) must be updated including supervisor requirements, assessing new security measures that will be applied to processing personal data (according to risk impact assessment).

d. Security document and risks analysis:

So far, companies had a "Security Document" on Data Protection, including all the measures and action protocols applicable therein in order to preserve data integrity and security.

The GDPR does not expressly require having this "Security Document" but indicates that companies should analyze risks and deficiencies or vulnerabilities that they can suffer, to select and implement the best solutions (technical or organizational) able to prevent, stop or neutralize attacks.

The result of this Risks Analysis can be reported and the "Security Document" remains certainly an useful tool at this respect, even though it is still necessary to adapt and modify it as security standards (low, medium, high) do not exist anymore. Hence analyzed if security measures adapt to the GDPR requirements, every company will apply security measures according to the risks analysis and treatment register.

e. Communication protocols for personal data breaches to control Authority:

In contrast to the previous legislation in which breaches register was an internal tool of companies, the GDPR requires them to communicate breaches to control Authority and concerned persons within 72 hours, according to the seriousness and affection of rights violated.

Therefore, companies must set up effective proceedings and protocols to comply with this obligation.

2. Record of processing activities:

The record of processing activities represents one of the innovations of the GDPR; companies must precisely identify and incorporate in the internal record detailed information about data processing and data flows carried out and the accomplished compliance activities with the regulation. This information should be at control Authority disposal by request.

The record of processing activities will allow complying with regulation, ensuring an effective control over personal data treated and spotting easily processing risks.

3. Data protection impact assesments:

Although the GDPR does not set security levels as the previous Spanish Law on data protection did, it asks for an impact assessment in case of data processing characterized by high risks to violate rights and freedom of interested persons or if it is needed a systematic assessment of personal data, profiling, etc. and in other cases that Spanish Data Protection Agency will determine.

4. Designation of the Data Protection Officer (DPO):

Until now the security officer has been in charge of coordinating the implementation of all security measures in companies that treat middle- and high-level personal data. With the new GDPR, there will be a Data Protection Officer, who will assume coordination and control tasks in complying data protection companies' policies.

The Data Protection Officer will be necessary for entities and public bodies, as well for the private companies that treat personal data requiring large-scale systematic monitoring or particularly sensitive data on a massive scale.

According to Spanish draft bill on data protection, the following corporations should be required to design a data protection officer:

- Insurance and reinsurance entities.
- Distributors and retailers of electricity or natural gas.
- Entities managing information credit systems
- Entities managing advertising activities that involve analysis of preference or profiling.
- Health centers.
- Educational centers providing official education, universities, etc.
- Professional associations.
- Gaming companies.

Although a company is not formally obliged to design a Data Protection Officer, it could be highly recommended depending on its size, in order to improve compliance with data protection law and reduce treatment risks as the officer aims to inform, supervise and advice about protection data law compliance activities. Having a Data Protection Officer represents without any doubt a quality label for companies and increases their competitiveness.

OUR SERVICES:

AGM Abogados can support you in all the adaptation process due to our wide experience, technical and legal training in Data Protection issues:

1. Previous analysis of data treated by your company.
2. Reviewing and adjustment of consent/data forms and data processing contracts.
3. Updating of security measures and proceedings, designing and adjusting them according to risk assessment and GDPR requirements.
4. Employees training in data protection issues in order to allow them to manage data treatment and raise their awareness about data protection.
5. We can be your Data Protection Officer or we can also advice the internal officer designed by your company.
6. Continuous updating of legal requirements in data protection issues.

Contact us!
We can help you