ioannides demetriou LLC

EU General Data Protection Regulation (GDPR)

In the era of rapid technological developments and globalisation in which personal data is being collected and shared worldwide, with several businesses relying on online profiling on the basis of data collected, it has become increasingly important to safeguard individuals' privacy by giving individuals control over their personal data and by simplifying the regulatory environment for businesses. The EU has decided that this will be achieved through the enactment and implementation of a pan-European regulation - the General Data Protection Regulation (GDPR). Regulations are directly applicable in all member states without the requirement of the passing of enabling legislation by the member states.

This article provides an overview of the main features and the effect of the GDPR. It is intended as an introduction and does not constitute legal guidance or advice, for which suitably qualified lawyers should be consulted.

The GDPR will be enforced on the 25th May 2018 throughout the member states of the EEA. The new framework provides a higher level of protection of personal data by increasing the obligations of those who process personal data whilst strengthening the rights of individuals whose data is being processed. A vast number of organizations will be affected by the GDPR and as such, they should take immediate steps to prepare for compliance with the new regulation.

Who does the GDPR apply to?

The GDPR applies to all organisations within the European Union and organisations of third countries which are trading with the European Union, including private and public organisations, courts and judicial authorities processing of personal data.

What you need to know

What are personal data and special data?

The term personal data refers to any personal information which can be used to identify an individual, directly or indirectly, including the individual's name, email address, place and date of birth, telephone number, etc., whereas the term special data refers to sensitive information such as data revealing racial or ethnic origin, political opinion, religious or philosophical beliefs, genetic data, biometrics, health, criminal convictions etc.

ioannides demetriou LLC

When does a Data Protection Officer (DPO) need to be appointed?

The appointment of a DPO on an organisation is mandatory where (i) the processing is carried out by a public authority (ii) the processing organisation's main activities include monitoring of individuals systematically and on a large scale or (iii) the processing organisations process special categories of data on a large scale. Organisations which do not satisfy the above thresholds may appoint a DPO on a voluntary basis, and such appointments are encouraged by the authorities.

What are the main duties of a DPO?

A DPO is responsible for the following: to advise the processor of data (the organization) on the various technical and organizational measures that the processor should take to ensure compliance with the provisions of the GDPR, to provide assistance to individuals wishing to exercise their rights, for the education of the staff, and for communication and co-operation with the regulatory authorities. In Cyprus the Regulatory Authority is the Commissioner for the Protection of Personal Data. To facilitate his duties, a DPO should participate in management meetings, have full access to the facilities of the processing organization and be aware and involved in the creation of the Data Storage and Data Protection policies of the processor.

Who can be appointed as a DPO?

The DPO should have sufficient detailed knowledge of the GDPR and may either be employed directly by the processor or provide such services under a service contract. In the course of appointing a DPO, it is important for the organization to ensure that the tasks and duties of DPO do not result in a conflict of interest.

What are the main principles for processing of personal data?

The GDPR introduces the 'Principle of Accountability' on the basis of which processing organisations should at any time be able to demonstrate their compliance with the provisions of the GDPR. In this respect organisations should implement appropriate technical and organisational measures and should review and update such measures every three years or when risk in relation to the rights and freedoms of the data subjects is jeopardised or significantly increased. The main obligations in this respect include the following:

1. Conducting a data protection impact assessment in the case of high risk processing;
2. Formulating and implementing a data protection methodology by design and by default to integrate the necessary safeguards and protect the rights of data subjects;
3. Maintaining documentation and records relating to the processing carried out, such as a written record of processing activities.

The Principles of lawfulness, fairness and transparency continue to apply under the GDPR, as does the purpose limitation principle, the data minimisation principle and the accuracy principle, storage principle and integrity and confidentiality principle.

What is the role of consent under the GDPR?

Under the GDPR, consent has been given a central role providing a valid legal ground for processing of personal data. The rules for obtaining consent have however become stricter and now require that consent must be freely given, specific, informed and unambiguous. Any request for consent should be in clear and plain language and separate from other matters. Data controllers will be required to be able to demonstrate that consent has been given and organisations which already implement a consent system should ensure that those consents are reviewed to ascertain that they meet the new conditions, as should fair processing notices.

What are the rights of individuals?

One of the main aims of the EU in enforcing the GDPR was to significantly enhance the rights of individuals

whose data is being processed. The GDPR includes a number of rights such as the right of individuals to be accurately informed about the processing of their data including the purpose and possible period of processing, the recipients of personal data, the logic in automatic personal data processing and the consequences of such processing. Data subjects are given access rights to their personal data, along with the right to rectify incorrect data, the right to restrict processing in some cases or to object to processing for direct marketing purposes, the right to receive personal data concerning the subject in a commonly used, machine readable and interoperable format for transmission to another controller.

Perhaps the most contentious right which is now established is the right of data subjects to be forgotten, allowing individuals to request that their data is erased without undue delay if such data is no longer necessary for the purpose for which they were collected or processed, where a data subject has withdrawn its consent or objects to the processing of personal data concerning him or where the processing does not comply with the GDPR.

Do the supervisory authorities have any substantial powers under the GDPR?

The supervisory authorities have investigative and corrective powers. Specifically, their powers include, without limitation, authority to carry out data protection audits, notify controllers and processors of alleged infringements of the Regulation, issue warnings and reprimands to controllers and processors, order compliance with the GDPR, order communication with the data subjects in case of breach, impose limitations or bans on processing, order rectification or erasure or withdraw a certification and impose steep administrative fines.

Administrative fines are able to be imposed in addition to or in substitution of the measures mentioned above, taking into account the parameters of each case. Penalty amounts depend on the infringement in question with a cap equivalent to the greater of (i) up to 4% of the annual worldwide turnover of the controller or processor, or (ii) Euro 20 million.

In light of such severe fines, businesses have all the more reason to ensure compliance with the GDPR, as infringement would be quite an expensive risk to take.

How we can help you prepare for and implement the GDPR

The GDPR is the most significant change in the field of data protection in the last decades and it is crucial that those affected by the change fully understand and prepare for such changes with the support of a legal expert, not only to avoid any harsh sanctions but also to gain a competitive advantage in a market where due to the vast flow of personal data individuals and organisations have come to value the protection of their personal information more than ever.

The GDPR has direct effect and therefore creates a direct legal obligation on your organisation. May is just around the corner, and no extensions will be granted

Ioannides Demetriou LLC have assembled a suitably qualified and trained team to assist you in your GDPR preparation and compliance by assisting you with the following:

- Review or draft data protection policies in line with the GDPR;
- Review or draft Binding Corporate Rules, consents, forms, processing notices, Binding Corporate Rules, etc.;
- Provide advice on the lawfulness of data processing as carried out by your organisation;
- Consider the business relationship and review relevant contractual documentation between your organization and external data processors (e.g. I.T. firms) and advise in order to ensure that they are in line with the GDPR;

- Provide advice on the need of a Data Protection Impact Assessment on the basis of the activities of your organization and assist with its preparation where needed;
- Provide advice on data protection matters, such as data security breaches and transfers of data to third countries;
- Liaise with the Data Protection Authorities on behalf your behalf and arrange/assist with all required filings;
- Represent the client in any judicial proceedings relevant to data protection matters.
- We can work with your internal IT team and third-party providers of software and Data Protection audits and assessments or we can assist you to choose who to entrust the above tasks to. Our role is that of the legal adviser who is by your side in order to ensure that you are compliant and in time.
- It is important to note that Cyprus as a country has been late to realise the significance of the GDPR. This is however not an excuse for non-compliance. It is clear that unless a business can demonstrate that it complies with the GDPR not only will it risk penalties by the regulator but it will also be at risk in the conduct of its business. Third parties dealing with your organisation as customers or providers of a service are obliged by the GDPR to ensure that any data that they pass on is being passed on to an organisation that also complies with the GDPR. The effect of this requirement in such industries as hotels and tourism, public utilities and financial institutions is immense and must be dealt with if business with such third parties is to continue as normal after May 2018.

Ioannides Demetriou LLC
The City House, 17-19 Themistocli Dervi Street, 1066 Nicosia,
P.O. Box 20106, 1601 Nicosia, Cyprus
T. +357 22022999 F. +357 22022900
E. info@idlaw.com.cy