ANTONIOU
McCOLLUM
&CO.

GDPR: A New Data Protection Landscape

September 2017

ANTONIOU McCOLLUM &CO.

The GDPR

The inconsistent compliance requirements between Member States as well as different standards of interpretation and enforcement, the exponential impact of new technologies impacting the management of personal data since the mid-90s are largely the factors that led to the need for a new data protection regime in the EU.

The General Data Protection Regulation (EU) 2016/679 of 24 May 2016 (the "**GDPR**") is a technology-neutral regulation that enters into force in all Member States without the need for national transposition, and will therefore harmonise data protection across the EU.

Companies will now have consistent data protection compliance requirements across the EU.

The GDPR also gives national data protection authorities greater powers of enforcement, with harsh fines for regulatory infringement and increased litigation risk arising from aggrieved data subjects.

The GPDR is applicable as of 25 May 2018.

Key changes

Increased Territorial Scope

The GDPR has extra-territorial applicability and applies to all companies processing personal data of data subjects residing in the EU, regardless of a company's location.

A controller or processor not established in the EU is caught by the GDPR where its processing activities:

- relate to offering goods or services to data subjects in the EU (irrespective of whether payment is required) or
- are related to the monitoring of their behaviour (to the extent such behaviour takes places within the EU).

In such a case, the controller or processor must designate in writing a representative in the EU.

Penalties

The GDPR takes a tiered approach to fines. Organizations in breach of the GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater).

Consent

Consent must be as easy to withdraw as it is to give.

Conditions for processing based on consent of data subjects have been strengthened, transparency is increased and 'assumed consent' models are redundant under the GDPR.

Requests for consent must be given in an "*intelligible and easily accessible form, using clear and plain language*", with the precise purpose for the intended data processing attached to that consent.

The GDPR expressly states that when assessing whether consent is freely given, account will be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is unnecessary for the performance of that contract.

Breach notification

Under the GDPR, notification of personal data breaches by the controller to supervisory authorities is mandatory where the data breach is likely to "*result in a risk for the rights and freedoms of individuals*".

Notification must be made within 72 hours of the controller becoming aware of the breach.

Controllers must also notify data subjects "without undue delay" on becoming aware of a data breach.

Right to access

The GDPR gives data subjects the right to obtain confirmation from a data controller of whether or not his/her personal data is being processed and, if it is, the location and for what purpose.

Right to be forgotten

The right to be forgotten entitles the data subject to obtain from the data controller the erasure of his/her personal data.

The grounds on which this right can be invoked include where the purpose for which the data was collected is no longer applicable and where the data subject withdraws their consent to processing.

Data Portability

The GDPR introduces the data subject's right to data portability allowing the data subject (in certain circumstances) to request from a controller that personal data which has previously been provided to a controller be provided in a '*commonly used and machine readable format*'.

The data subject may then freely transmit such data to another controller.

Privacy by design

Privacy by design, a concept adopted by more sophisticated controllers for some time, is now a mandatory under the GDPR.

Article 25 requires that controllers expressly consider (both at the time of determining the means for processing as well as at the time of processing) the implementation of appropriate operational and technical measures designed to implement data protection principles and have as their objective the requirements of the Regulation to protect the rights of data subjects.

Article 25 specifies that the measures that controllers implement should ensure that, by default, only personal data necessary for each specific purpose of the processing are processed. This obligation applies to:

- The amount of data collected
- The extent of processing
- Their period of storage
- Data accessibility

Article 25 expressly states that the measures shall ensure that by default, personal data are not made accessible *without the individuals' intervention* to an indefinite number of natural persons.

Data Protection Officers

The DPO is perhaps one of the most significant changes under the GDPR for organisations that previously were not required to nominate one under the laws of the applicable jurisdiction.

Under the GDPR, DPO appointment is mandatory for those controllers and processors where:

- Processing is carried out by a public authority or body (except courts);
- the core activities of the controller/processor consist of processing operations which require regular and systematic monitoring of data subjects on a large scale; and
- the core activities of the controller/processor consist of the processing on a large scale of special categories of data or data relating to criminal convictions and offences.

The DPO:

- must be appointed on the basis of professional qualities and, in particular, expert knowledge on data protection law and practices;
- may be a staff member or an external service provider;
- may be appointed by a group of undertakings;
- contact details must be communicated to the relevant DPA;
- must be provided with appropriate resources to carry out his/her tasks and maintain expert knowledge
- must report directly to the highest level of management; and
- must not carry out any other tasks that could results in a conflict of interest.

Conclusion

The GDPR is a complex area of legal compliance which has ramifications for all companies with activity in the EU, regardless of whether their operations are based within the EU or elsewhere.

The GDPR is wider in scope than its predecessor and by 25 May 2018 businesses caught by the GDPR must have undertaken self-assessments, audits, compliance paper trails and the like to ensure compliance.

Our expertise

We specialise in Cyprus and EU data protection laws and advise companies on all legal aspects of data compliance.

Contact us to discuss your precise requirements.