General Data Protection Regulation (**GDPR**) (Regulation (EU) 2016/679).

The GDPR was enacted by the Council of the European Union and the European Commission on April 14, 2016 and will be directly applicable in all Member States by 25 May 2018.

The GDPR replaces the Data Protection Directive no. 95/46/EC and aimed at harmonizing data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

The key points of the GDPR as well as information on the impacts it will have on business is briefly listed below:

(i) Extra-territorial applicability

The biggest change to the regulatory landscape of data privacy comes with the extended jurisdiction of the GDPR, as it applies to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to: offering goods or services to EU citizens and the monitoring of behaviour that takes place within the EU. Non-Eu businesses processing the data of EU citizens will also have to appoint a representative in the EU.

(ii) Breach Notification

Under the GDPR, breach notification will become mandatory in all Member States where a data breach is likely to "result in a risk for the rights and freedoms of individuals". This must be done within 72 hours of first having become aware of the breach.

(ii) Right to Access

The GDPR entitles data subjects to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Furthermore, the controller shall provide a copy of the personal data, free of charge, in an electronic format.

(iii) Data erasure

The so-called "right to be forgotten" entitles the data subject to have the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties stop processing of the data.

(iv) Data Portability

GDPR introduces data portability, i.e. the right for a data subject to receive the personal data concerning them, which they have previously provided in a "commonly use and machine readable format" and have the right to transmit that data to another controller.

(v) Privacy by Design

Privacy by design is a legal requirement with the GDPR. It calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

(vi) Data Protection Officers (DPO)

Under GDPR it will not be necessary to submit notifications / registrations to each local Data Privacy Authorities of data processing activities. Instead, there will be internal record keeping requirements, as further explained below, and DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale,

or of "Special categories" of data (including information such as health data or religious and political beliefs).

(vii) Penalties

Under GDPR, organizations in breach of data protection Regulation can be fined up to 4% of annual global turnover or € 20 Million (whichever is greater). This is the maximum fine that can be imposed for the most serious infringements (e.g. not having sufficient customer consent to process data or violating the core of Privacy by Design concepts). There is a tiered approach to fines: e.g. a company can be fined 2% for not having their records in order (article 28), not notifying the supervising authority and data subject about a breach or not conducting impact assessment.

Feel free to contact me with any issues arising from the foregoing.

Best regards,