INTRODUCTION

The **General Data Protection Regulation** (GDPR) is an EU (European Union) Regulation which came into force in EU member states on May 25th, 2018. It replaces the former EU Directive 95/46/EC and extends its scope and reach. It covers the **processing of personal data by EU establishments** for the geographic scope as below. Despite being a Regulation, it allows member states to legislate in many areas which will be a challenge to overall GDPR consistency. Certain activities such as matters of law enforcement agencies and national security are excluded from the GDPR.

KEY CONCEPTS

Data Controller - A person or body, alone or jointly, which determines the purposes and means of processing personal data.

Data Processor - An entity which processes the data on behalf of the data controller.

Personal Data - This is any information relating to an identified/ identifiable, natural person, a 'data subject'. A sub-category is 'sensitive data' covering issues such as biometric records.

Data Subject - a natural person, who can be identified, or is identifiable, directly or indirectly.

Processing - This is defined widely to cover any operation or set of operations which is performed on personal data or sets of personal data, whether by automated means or otherwise. Examples of processing include the collection, recording, organisation, storage, use and destruction of personal data.

Geographical Scope: An EU based data controller and processor falls into the GDPR scope where personal data is processed *"in the context of its activities"* - a broadly interpreted test. Where no EU presence exists, the GDPR will still apply through Article 3 whenever: (1) an EU resident's personal data is processed in connection with goods/services offered to him/her; or (2) the behaviour of individuals within the EU is "monitored".

Consent – Consent is an important, yet not the only lawful basis for processing a data subject's personal data. For consent to be valid it must be **freely given,** and the data subject informed with regards to the identity of the controller and the purposes of the processing. Automated or all-encompassing consent is not allowed. Further, the data subject can withdraw consent at any time. **Children under the age of 13 can never give consent** by themselves and parental consent is required. Between the ages of 13 – 15 there is some leeway for member state legislation.

Pseudonymisation – a processing technique by which the data can no longer be related to a specific data subject without the use of additional information. GDPR allows for this technique to be used e.g. as part of a '**data privacy by design**' approach which includes staff training and data minimisation.

Accountability – data controllers are responsible for demonstrating compliance with the data protection principles.

Rights of the Data Subject - these include the right to be 'forgotten' (erasure and destruction of personal data), the right to request the porting of one's personal data to a new organisation, the right to object to certain processing activities and to decisions taken by automated processes.

Notification for Personal Data Breaches – data processors to report breaches to their data controllers and data controllers to report breaches to their supervisory authority no later than 72 hours after becoming aware of a breach. Non-compliance can lead to an **administrative fine up to €10M/€20M** or in case of an undertaking,

up to 2%/4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.
Codes of Conduct – GDPR makes provision for 'best practice' to support data controllers and processors meet compliance requirements.
Transfers of Personal Data – outside of the European Economic Area (EEA) may only take place if the country has obtained an adequacy decision by the European Commission (EC), other appropriate safeguards such as Binding Corporate Rules are in place, or the law allows the transfer for a specific situation. The EC maintains a list of approved countries.
Remedies for Data Subjects – right to lodge a complaint with a supervisory authority, obtain judicial relief, get compensation for material or immaterial damage by a data processor or data controller, make claims for non-pecuniary loss, participate in class actions and appeal a verdict.
Liability - this applies to both data controllers and data processors for infringement and judicial remedies.
Supervisory Authorities – national data protection authorities will continue to exist, will co-operate with the EU and must act independently.
European Data Protection Board - an EU body with a legal personality and extensive powers to determine disputes between national supervisory authorities, to give advice and guidance and to approve EU-wide codes and certification.

KEY PRINCIPLES

The processing must be **Lawful, fair and transparent**, i.e. the data subject is to be provided access to details about the processing, **limited** to necessary activities, and **accurate.**
Data must only be collected for an **explicit and legitimate purpose**,
kept in **storage for no longer than necessary** and
conform to **integrity and confidentiality** requirements.
Data Governance - requires all organisations to implement a wide range of measures to reduce the risk of their breaching the GDPR. This may include the appointment of a **Data Protection Officer** (DPO).

DISCLAIMER

This document provides only a high-level overview of the GDPR for the layman. It makes no claims and disclaims all liability for completeness and accuracy.

Contact Information

CCube Consulting GmbH
Bertrand George
Managing Director
Mobile +41 79 238 62 44
bertrand.george@ccube.ch
www.ccube.ch
8707 Uetikon am See,
Switzerland