General Data Protection Regulation
25 May 2018

What is the GDPR?

The General Data Protection Regulation (GDPR) represents the most important reform of EU data privacy for over 20 years, it is effective from May 25th 2018. The GDPR:

- Aims to protect fundamental rights and freedoms of individuals and gives them better control over their personal data.
- Requires entities to be able to demonstrate ongoing compliance (principle of accountability).
- Imposes greater sanctions in case of non-compliance with the GDPR.

Who must apply this new regulation?

All entities within the European Economic Area (EEA) and entities outside the EEA that process personal data of individuals who are in the EEA to offer them products/services or monitor their behaviour.

What is personal data?

Personal data is any information related to an identified or identifiable individual (e.g. name & ID, transactional data, family situation, e-mail, IP address, etc.). Some personal data are sensitive such as: health and biometric data, ethnic origin, religious or philosophical, etc. and may not be collected without the individual's consent.

What individuals are concerned?

All individuals are concerned by the GDPR: individual clients, prospects, company's representatives, employees, supplier's representatives, Ultimate Beneficial Owners.

What is a processing of personal data?

A processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means (collect, record, store, consult, disclose, erase, archive).

What are the personal data protection principles?

Each and every processing of personal data must comply with the following principles: Lawfulness & fairness, purpose limitation, data minimisation, storage limitation, security, accuracy and transparency.

- Transparency towards individuals is key for the Group. Individuals must be informed on what personal data we use, for what purposes and with whom we share it with.

What are the individuals' rights?

- The GDPR strengthens the existing rights: the right to information, access, object and rectify. It also creates new ones: the right to restrict processing, erasure, not to be subject to an automated decision making and the right of data portability.

What does accountability with the GDPR means?

- **Governance set-up:** establishment of a clear governance within the Group and appointment of a Data Protection Officer (DPO). One of his role, is notably to supervise the ongoing compliance with personal data protection regulations and Group procedures
- **Privacy by design:** Personal data protection matters must be considered and integrated in all products, services, IT systems, projects, processes from the earliest stage and through their entire lifecycle.
- **Privacy Impact Assessment (PIA):** You have to verify if a deeper analysis must be performed where a high risk to the privacy of individuals may exist.

§ **Record of processing:** records of processing activities must be kept by entities to be able to demonstrate compliance.

How does the GDPR impact services providers?

§ The GDPR imposes direct compliance obligations on services providers.
§ Both the service provider and the Group entity may be liable towards individuals. A written contract is necessary between the parties

What are the impacts of the GDPR on cross-border transfers?

§ The GDPR prohibits transfers (including access) of personal data from entities located in the EEA to entities located outside the EEA that do not provide an adequate level of protection unless certain safeguards are in place (e.g. EU clauses, BCRs).

What is a personal data breach?

§ A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

§ All relevant stakeholders such as CDO, IT, CSIRT, LEGAL, RISK, Compliance, Business and Communication must be involved in the data breach management. The DPO has 72 hours to notify certain breaches to Data Protection Authorities. When a personal data breach is likely to result in a high risk to the rights and freedom of individuals, the affected individuals must also be notified.
§ Non-compliance with the GDPR could lead to reputational damages, loss of customers' trust and financial sanctions up to 4% of global annual turnover.

What are the best practices in terms of personal data breach prevention to keep in mind?

§ Do not open, response or forward emails which contain personal data if you do not trust in the source

§ Always store and process personal data in the Group environment in line with the local applicable policy
§ Do not store personal data in a local or shared folder unless there is an approved business need
§ Install only the Group's authorized software in your devices
§ Ect…