GDPR Key Changes Handout

The following document was created from the website: https://eugdpr.org/the-regulation/.
All text was taken from this website, not created by the DIGIT partnership.

The aim of the GDPR is to protect all EU citizens from privacy and data breaches in today's data-driven world. Although the key principles of data privacy still hold true to the previous directive, many changes have been proposed to the regulatory policies; the key points of the GDPR as well as information on the impacts it will have on business can be found below.

Increased Territorial Scope (extraterritorial applicability)

- Arguably 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 Union, regardless of the company's location.
- Previously, territorial applicability of the directive was ambiguous.
- The GDPR also applies 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 (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the EU.

Penalties

- Organizations in breach of GDPR 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.

Consent

- The **conditions for consent have been strengthened**, and companies are no longer able to use long illegible terms and conditions full of legalese.
- The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent.
- Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language.
- It must be as easy to withdraw consent as it is to give it.

Breach Notification

- Under the GDPR, breach notifications are now 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. Data processors are also required to notify their customers, the controllers, "without undue delay" after first becoming aware of a data breach.

Right to Access

- Part of the expanded rights of data subjects outlined by the GDPR is the right for data subjects to obtain confirmation from the data controller as to whether or not personal data concerning them is being processed, where and for what purpose.
- Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format. This change is a dramatic shift to **data transparency** and empowerment of data subjects.

Right to be Forgotten

- Also known as Data Erasure, the 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 halt processing of the data.

Data Portability

- GDPR introduces data portability – the right for a data subject to receive the personal data concerning them.

Data Protection Officers

- Under GDPR it is not necessary to submit notifications / registrations to each local DPA of data processing activities, nor is it a requirement to notify / obtain approval for transfers based on the Model Contract Clauses (MCCs).
- Instead, there **are internal record keeping requirements**, as further explained below, and DPO (Data Protections Officer) appointment is mandatory only for those 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 or data relating to criminal convictions and offences.**
- Importantly, the Data Protection Officer:
  - 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
  - Contact details must be provided to the relevant DPA
  - Must be provided with appropriate resources to carry out their tasks and maintain their expert knowledge
  - Must report directly to the highest level of management
  - Must not carry out any other tasks that could results in a conflict of interest.

Please consider the following questions:

1. What do you think about these guidelines? What stands out for you?
2. Have you been affected by these in your personal or professional life? If so, how?
3. Is there anything else you would add or change about the GDPR regulations?