HUM 4441
ENGINEERING ETHICS

Dr. Mohammad Rezwanul Huq

Adjunct Faculty, IUT

EU GENERAL DATA PROTECTION REGULATION (GDPR)

GDPR

- A regulation (set of rules) drafted by the EU. All EU Member States must follow these rules.
- It sets out rules for data protection and privacy for all individuals within the EU.
- The GDPR includes rules for how physical or legal persons may process personal data.

PURPOSE OF GDPR

- The purpose of the regulation is to create a uniform and harmonised level of protection for personal data within the European Union. So the free movement of personal data within Europe is not limited.

DEFINITION OF PERSONAL DATA

- Personal data means any information which, directly or indirectly, could identify a living person. Name, phone number, and address are schoolbook examples of personal data. Interests, information about past purchases, health, and online behaviour is also considered personal data as it could identify a person.
- "Any information relating to an identified or identifiable physical person ('data subject') (i.e. not a legal entity); an identifiable physical person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." [Article 4(1), GDPR]

PROCESSING PERSONAL DATA

- Processing data means collecting, structuring, organizing, using, storing, sharing, disclosing, erasing and destruction of data.
- **Each organization that processes personal data (which is every organization with employees and customers) must ensure that the personal data it uses fulfils the requirements of the GDPR.**

REQUIREMENTS OF GDPR

- Same law throughout Europe.
- Use personal data must in line with integrity friendly principles.
- Use of personal data must be legal.
- Use of personal data must be respectful to the individuals' rights.
- Personal data breaches must be reported within 72 hours.
- Businesses are responsible for their suppliers.
- The size of the sanctions are significant.
  - Organisations that violate the law may face sanctions of up to the higher amount of 4% of their global sales (the last 12 months) or € 20 million.

WHY GDPR?

- **Personal data is valuable.**
- Data makes it possible to develop business models, gain an understanding of its customers, conduct effective marketing campaigns and develop its products and services.
- But just as for many other assets, there is a need for responsible use based on common rules. The last few years we have seen headlines of personal data breaches and scandals from Facebook, eBay, Equifax and Uber. Hundreds of millions of individuals' personal information (social security numbers, addresses, credit scores, etc.) were compromised.
- The GDPR not only clearly states that an individual's personal data belongs to the individual; it also threatens to impose substantial fines for companies not following the rules.
- In Europe, privacy and data protection are considered vital components for a sustainable democracy. The GDPR is designed to safeguard these prerequisites and is an upgrade of the past EU data protection directive.

PRACTICAL IMPLICATIONS

- Inform citizens and customers of your activities in a transparent manner.
- Assign a Data Protection Officer (DPO) to your organisation who should work as the main operator and the expert on your organisations' privacy work.
- Manage the citizens' and individuals' rights efficiently.
- Regulate the responsibility between Buyer (Controller) and Supplier (Processor).
- Keep a data inventory.
- Set up processes to manage personal data breach within a 72-hour time frame.
- Analyze possible risks and impacts on citizens' rights for the intended use of personal data.