**LECTURE 5 🡪 PRIVACY AND PRIVACY ENHANCING TECHNIQUES**

There is no clear definition of what is privacy, but a good definition can be used (within the data context) **legal control over access to and use of data stored in computers**

A more generic one would be the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others

PRIVATE is registered in the ‘human rights’

Privacy dimensions

1. Data protection privacy

* *Information privacy* 🡪 the right to control how and whether their data is collected, stored, processed and disseminated
* *Privacy of communications* (e.g. whatsapp, emails, …)

1. Beyond data protection-related privacy

* Spatial privacy (virtual space, e.g. hacking)
* Territorial privacy (physical area)
* Bodily privacy (protection of individuals physical body against certain procedures)

Privacy vs Security

Security triad 🡪 CIA (conf, integrity, availability)

Privacy protection goals are though CIA +

* Unlinkability (data cannot be linked across different domains). E.g. I have data in one system (Netflix) but
* Transparency 🡪 access to information about data
* Intervenability 🡪 you should be able to intervene (I DON’T WANT MY DATA TO BE PUBLISHED)

There are some standards and regulations

GDPR 🡪 general data protection and regulation (since 2018)

Objectives:

* Harmonization of data protection (same laws for every country)
* Modernization of data protection rules (stay ahead of technology)
* Make citizens have more power and more control
* Improve level of compliance (can comply easily)

Affects all EU members states, and also deals with data leaving the EU.

Also, there are exceptions like criminal law, public security, etc.

**What is personal data?**  
Any information that relates directly or indirectly to an alive person

This information is encrypted may be used for reidentification of an individual. E.g. location, photos, IP address, personal email, …

If it is anonymized, it is no longer personal data

**What is sensitive personal data?**

* Political data
* Ethnic or racial origin
* Philosophical or religious beliefs
* Health and sex life related topics

It is **forbidden** to process sensitive data unless consent is obtained from data subjects or owners

**What is data processing?**

Collecting, recording, storing, organising, structuring, alteration, dissemination, etc. Examples are sensors, promotion through email, video recording.

GDPR 🡪 what are the rights of citizens?

* Right to be **informed** about actions on your data
* Right to **access** your data
* Right to **rectification** of data
* Right to **remove** data of yours (right to be forgotten)
* Right to **restrict** processing
* Right for **using** one’s data
* Right to object against the use of personal data by other entities (say no to marketing)
* Right to profiling an automated version

Taxonomy of Privacy (**IMPORTANT)**

The taxonomy of privacy will enable you to identify *potential harms* arising from infringements of privacy

4 group of activities:

1. Information **collection** (cameras (*surveillance*), *interrogation*)
2. Information **processing** (*aggregation* – combining data -), *identification* … can they use the information they gathered from you? *Insecurity, secondary use, exclusion* …
3. Information **dissemination** (*breach of confidentiality, disclosure* to third parties*, exposure* of physical and emotional attributes*, increased accessibility, blackmail, appropriation* use your data for accessing a system …*, distortion* misleading info to others about you*)*
4. **Invasion** (*intrusion* into one’s life and *decisional interference* like the Brexit thing)

Privacy by Design

Privacy is a social construct, but data protection is tangible. The motivation for privacy for design are the following:

* Need to manage information responsibility has grown
* Privacy has evolved
* Privacy must be approached as being an integral part of systems
* Privacy must be embedded into protocols and processes that touch our lives.

**The 7 privacy design principles are:**

1. **Proactive** and not reactive, **preventive** and not remedial. That means anticipation of potential harming events, with high commitment. Use highest standards
2. Privacy as the **default setting**. Purpose specification, collection limitation, data minimalization (only important fields), use, retention and disclosure limitation.
3. Privacy **embedded** into the design. Wherever it is possible, use it. E.g. a new app must not access your camera
4. **Full functionality, positive sum**. Other requirements should not affect functionalities. All interests and objectives must be clearly documented
5. **End to end** security, full lifecycle protection. Privacy must be continuously protected across the entire domain. Conf, integrity and availability must be applied all the time
6. **Visibility & Transparency.** It is essential in order to establish accountability. Everything privacy procedure and policy should be documented, available, and compliance should be available.
7. **Respect for user privacy**. Keep it user centric, design based on individual users. Access, accuracy, compliance, user friendly

Privacy preserving techniques

Since protection of data is critical, technical solutions are needed to ensure data privacy

Some examples are regulations, standards, protocols, tools and mechanisms (encryption, anonymization, pseudonymization), data security and integrity, identity management

1:39:01