

LEGAL REGULATION IN SOFTWARE ENGINEERING

LEVEL 200 SOFTWARE ENGINEERING (WEEK 2)

CHAPTER FOUR

DATA PRIVACY LAWS AND GDPR

By Asick PECKINS



PLAN OF THE DAY

- Introduction to data privacy laws and regulations.
- Depth exploration of GDPR (General Data Protection Regulation) Process of obtaining copyright for software.
- Data subject rights and responsibilities of data controllers.
- Integrating privacy by design in software development.

INTRODUCTION TO DATA PRIVACY LAWS AND REGULATIONS

- ✓ Data privacy laws and regulations are designed to protect the privacy and security of personal information.
- ✓ These laws and regulations apply to both individuals and organizations that collect, store, and use personal data.

INTRODUCTION TO DATA PRIVACY LAWS AND REGULATIONS

- ✓ Personal data includes any information that can be used to identify an individual, such as name, address, social security number, email address, phone number, or IP address.
- ✓ Data privacy laws and regulations vary by country and region, but some of the most well-known include the General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada.
- ✓ These laws and regulations typically require organizations to obtain consent from individuals before collecting and using their personal data, provide individuals with access to their data, and implement security measures to protect against data breaches.

INTRODUCTION TO DATA PRIVACY LAWS AND REGULATIONS

- ✓ Failure to comply with data privacy laws and regulations can result in significant fines and legal penalties for organizations.
- ✓ As technology continues to advance and more personal data is collected and stored online, data privacy laws and regulations are likely to become even more important in protecting individuals' privacy rights.

Depth exploration of GDPR (General Data Protection Regulation) Process of obtaining copyright for software.

In 2018, the law concerning how personal data is treated by an organization was updated to take into account the huge amount of data that is now stored. This is known as the General data protection regulation 2018 and is broadly similar to the principles in the data protection Act 1998/2018, with a few amendments.

GDPR SPECIFIES THAT PERSONAL DATA MUST BE

- ✓ Processed lawfully, fairly and transparently, this means organizations need to tell people what data is being stored and what it will be used for including cookies on websites, online forms and apps
- ✓ Collected for specified, explicit and legitimate purposes-the data cannot be used for anything other than what it was originally collected for.
- ✓ Adequate, relevant and limited to what is necessary about the purposes for which it is processed - data cannot be collected that is not relevant to the organization's needs.

GDPR SPECIFIES THAT PERSONAL DATA MUST BE

- ✓ Accurate and , where necessary, kept up to date – individuals have the right to request that data is changed but it is also the responsibility of the organization to make sure that data is correct
- ✓ Kept in a format which identifies individuals for no longer than is necessary-data can be kept for longer as long as anything that identifies the individual is removed.
- ✓ Processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical

GDPR SPECIFIES THAT PERSONAL DATA MUST BE

or organisational measures in other words, an organisation must take adequate actions to ensure that the data is safe from accidental loss and cyber-attacks



RIGHTS AND RESPONSIBILITIES OF DATA CONTROLLERS

Data subject rights refer to the rights that individuals have over their personal data, including the right to access, rectify, erase, restrict, and object to the processing of their data.

The responsibilities of a data controller include

Ensuring that personal data is collected and processed lawfully, fairly, and transparently, implementing appropriate security measures to protect against data breaches, and responding to data subject requests in a timely manner.

The responsibilities of a data controller include

Data controllers must also appoint a Data Protection Officer (DPO) in certain circumstances, such as when processing sensitive personal data or conducting large-scale processing activities.

The responsibilities of a data controller include

It is important for organizations to understand their responsibilities as data controllers and to ensure that they are complying with all relevant data privacy laws and regulations to protect the privacy and security of personal data.

INTERGRATING PRIVACY BY DESIGN IN SOFTWARE

Privacy by design is an approach to software development that prioritizes privacy and data protection throughout the entire development process.

To integrate privacy by design, developers should consider the following:

- ✓ Conducting a privacy impact assessment (PIA) to identify potential privacy risks and develop strategies to mitigate them.
- ✓ Implementing privacy-enhancing technologies (PETs) such as encryption and anonymization to protect personal data.
- ✓ Limiting data collection to only what is necessary for the intended purpose.
- ✓ Providing clear and concise privacy notices and obtaining consent from users before collecting their personal data.

To integrate privacy by design, developers should consider the following:

- ✓ Ensuring that data is securely stored and transmitted.
- ✓ Regularly reviewing and updating privacy policies and procedures to ensure compliance with changing laws and regulations.



To integrate privacy by design, developers should consider the following:

By integrating privacy by design, developers can help protect the privacy and security of personal data, build trust with users, and avoid costly data breaches and legal consequences.