Makara Ramoabi

20240045

IT Law

1.Data protection

An app/website that operates using client/user data must adhere to strict data protection laws, these laws are meant to guide developers/businesses on how to access, manage, and interact with user data. It is also important to know which laws apply. The most important is to follow the core principles of data protection like; lawfulness, fairness, transparency; by disclosing how the data is going to be used via privacy policy.

Purpose limitation- by asking for relevant data (e.g. Name, Age, Email for log in purposes)

Storage limitation- keeping data for as long as it is needed (e.g. keeping inactive user data for a specified period)

Security- protecting user data (Using HTTPS for secure data transfer or encrypting user data)

All these steps must be taken in to consideration and implemented. Without any of these rules/guidelines being followed, it could lead to data breaches, unethical use of user data, and fines/lawsuits that could prevent further operation.

2.**Legal study**

The General Data Protection Regulation (GDPR) is an EU regulation that governs how personal data must be collected, stored, processed, and transferred. It mandates principles like lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality. In IT, GDPR forces system designers to build privacy into products (privacy by design), maintain strong security (encryption, access controls), manage data retention and deletion, implement consent mechanisms, support data subject rights (access, correction, deletion), and ensure proper oversight (data protection officers, audits).

3.**Case study**

In September 2024, Clearview AI was fined €30.5 million by the Dutch Data Protection Authority under GDPR. The company created a database of billions of facial images scraped from social media—many of them of Dutch citizens—without their consent. The Dutch DPA found multiple violations including use of biometric data (a special category under GDPR), lack of transparency, failure to inform people how their data was used, and failure to facilitate individuals' rights. Clearview was ordered to stop the illegal processing and may face further fines for non-compliance.

4. Compliance list