1. **Data Privacy**

Data privacy in AI and machine learning refers to the practices and measures taken to protect personal information from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves ensuring that individuals' personal data is handled responsibly and ethically, particularly as AI systems require vast amounts of data to function effectively.

**Example Use Case: Healthcare Data**

Consider a healthcare app that uses patient data to predict diseases. If the app collects and stores sensitive personal information without proper consent, it risks violating patient privacy.

**Ethical Consideration**: Implement strict data handling protocols, anonymize personal data, and ensure informed consent is obtained from users. Adhere to privacy regulations like GDPR.

**Mandatory Reading:**

Generative AI brings new data privacy challenges
https://teknologiradet.no/en/generative-ai-brings-new-data-privacy-challenges/