This presentation offers an overview of GDPR, emphasizing its importance in protecting personal data, particularly in research contexts. Here's a structured summary of the key points:

General Data Protection Regulation (GDPR)

- **Purpose: Protects individuals' personal data from misuse.**
- **Effective: EU-wide from 25 May 2018.**
- **Key Stakeholders:**
    - **Data Controller: Decides how and why data is processed.**
    - **Data Processor: Processes data on behalf of the controller.**
    - **Data Protection Officer (DPO): Ensures compliance.**
    - **Data Subject: The individual whose data is collected.**

Personal Data

- **Definition: Any data that identifies a person directly or indirectly.**
- **Categories:**
    - **General Personal Data: Name, ID number, location data, etc.**
    - **Sensitive Data: Racial/ethnic origin, political opinions, health, biometric data, etc.**
- **Processing Rules:**
    - **Requires explicit consent or a legitimate legal basis.**
    - **Must adhere to GDPR principles like data minimization and purpose limitation.**

GDPR Principles

1. **Fairness, Lawfulness, and Transparency: Data collection must be clear and justified.**
2. **Purpose Limitation: Use data only for specified purposes.**
3. **Data Minimization: Collect only what is necessary.**
4. **Accuracy: Keep data current and correct.**
5. **Storage Limitation: Retain data only as long as necessary.**
6. **Integrity and Confidentiality: Protect data with robust security measures.**
7. **Accountability: Ensure compliance and readiness to demonstrate adherence.**
8. **No Overseas Transfer: Without adequate safeguards.**

Data Anonymization and Pseudonymization

- **Anonymization: Removes all identifiers, making re-identification impossible.**
- **Pseudonymization: Separates identifiers from data with additional safeguards.**

Challenges in Research

- **Legal risks related to:**
  - **Data protection compliance.**
  - **Copyright violations.**
  - **Unintended discovery of criminal activities.**
- **Ethical dilemmas, such as using improperly obtained data.**

Case Studies

1. **Hard Disk Discovery: Using a found device risks processing stolen data—non-compliance.**
2. **Public Forums (Boards.ie): Open-access data may not always mean legal to use.**
3. **Ashley Madison Breach: Highlights risks in using protected networks without proper authorization.**

Considerations for Researchers

1. **Always ensure informed consent for data use.**
2. **Clearly define the purpose of data collection.**
3. **Anticipate data security measures in advance.**
4. **Avoid relying on "free online data" without checking legality.**

Real-World Example

- **Optus Data Breach (Australia, 2022):**
  - **Exposed personal details of ~10 million individuals.**
  - **GDPR-like regulations could have mitigated its impact.**

Resources

- **Citizens Information: Overview of GDPR**
- **Irish Data Protection Commissioner**

- DCU Data Protection Resources

This foundation prepares researchers to navigate GDPR's complexities, ensuring ethical and legal compliance in data handling.