THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU)

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

AIAA 2290: Ethics, Privacy and Security in AI

Foundations of Data Privacy

Xuming HU

xuminghu@hkust-gz.edu.cn

The Hong Kong University of Science and Technology (Guangzhou)

2025 Spring

1 Introduction to Data Privacy

2 Data Privacy Principles

3 Data Privacy Technologies

4 Data Privacy in Practice

5 Data Privacy Policies and Notices

6 Future of Data Privacy

01

Introduction to Data Privacy

What is Data Privacy?

Why Privacy Matters?

What is Data Privacy?

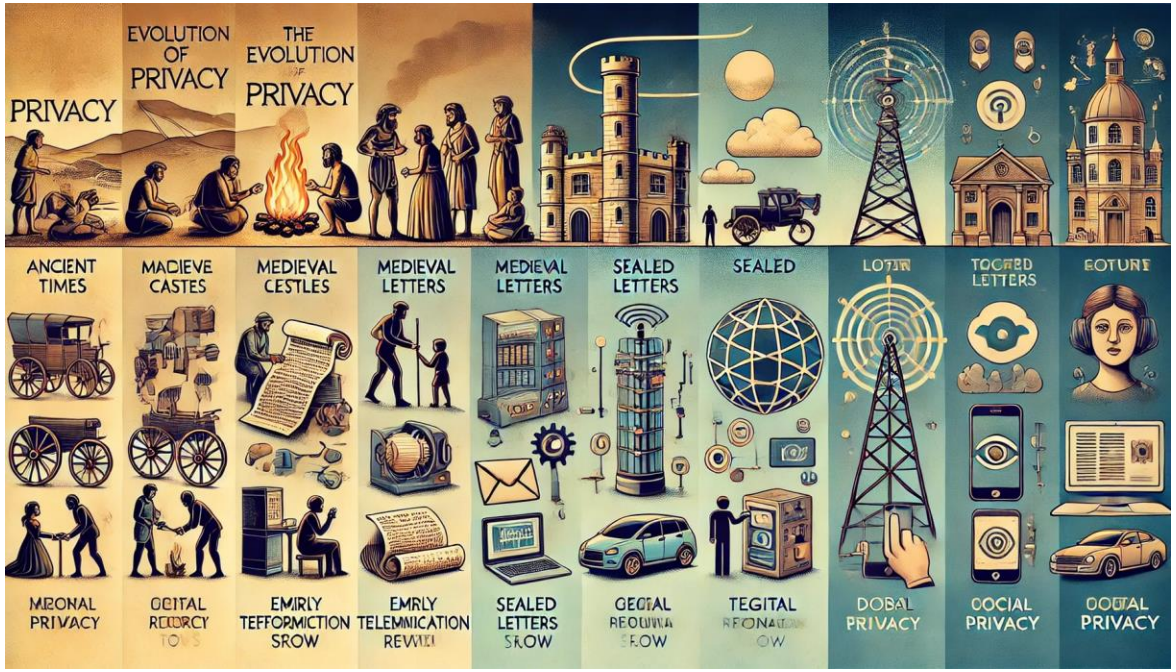
Data privacy refers to the protection of individuals' personal information from **unauthorized access, use, or disclosure.**

Why Privacy Matters

Privacy is a fundamental human right and a key component of personal autonomy. It matters because it protects individuals from potential harm, such as **identity theft, financial loss, and reputational damage.**

The Evolution of Privacy

The concept of privacy **has evolved significantly over time.**



Privacy in the Digital Age

The rise of social media, e-commerce, and smart devices has increased the vulnerability of personal information.

AI knowledge Quiz

In the digital age, the concept of privacy has become increasingly important.

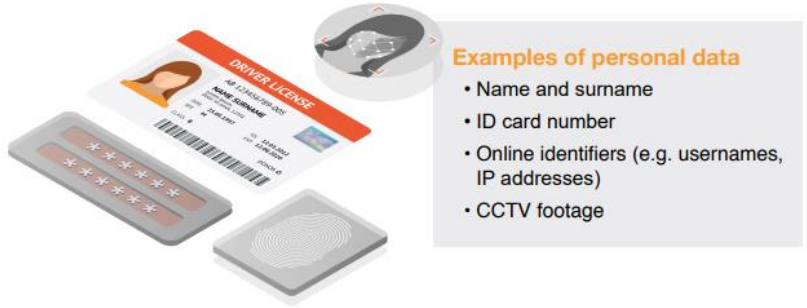
What do you think constitutes Personal Data? Explain your answer with examples.

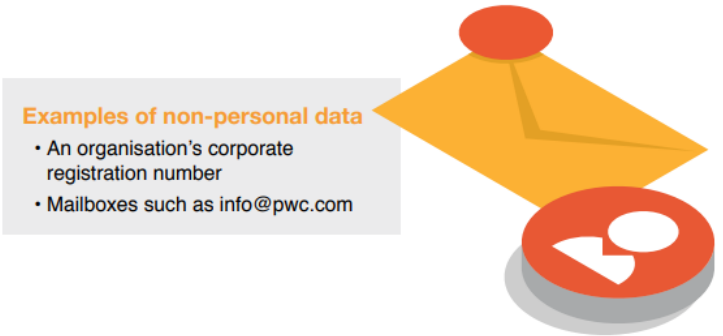
What is the difference between personal data and sensitive data?

Introduction to Personal Data

Personal Data refers to any information that can identify or be associated with a specific individual. According to various regulations (such as the **General Data Protection Regulation (GDPR)**), personal data typically includes the following categories:

- **Directly Identifiable Information**
- **Indirectly Identifiable Information**
- **Sensitive Information**





Some examples of Sensitive Data

Sensitive data is a subset of personal data.

AI knowledge Quiz

Which of the following is NOT considered Sensitive Data?

A) Health records

B) Race

C) Name

D) Sexual orientation

AI knowledge Quiz

If a person's health information is disclosed, it could severely affect their privacy or security. What type of data is this?

A) Personal Data

B) Sensitive Data

C) Not Data

D) Public Data

02

Data Privacy Principles

Definition

Data privacy principles ensure that the collection, storage, use, and sharing of personal data comply with laws and regulations, protecting individuals' privacy. Below are some key data privacy principles:

- **Lawfulness, Fairness, and Transparency**
- **Purpose Limitation**
- **Data Minimization**
- **Accuracy**
- **Storage Limitation**
- **Integrity and Confidentiality**
- **Accountability**

Definition

The principles are:

Lawfulness, fairness and transparency

You should always process personal data in a fair, lawful and transparent manner.

Purpose limitation

You should only process personal data for a specified and lawful purpose.

Data minimisation

You must ensure you are only processing the personal data that you truly need and nothing more.

Definition

The principles are:

Lawfulness, fairness and transparency

You should always process personal data in a fair, lawful and transparent manner.

Purpose limitation

You should only process personal data for a specified and lawful purpose.

Data minimisation

You must ensure you are only processing the personal data that you truly need and nothing more.

Accuracy

You should ensure personal data is kept up to date, and that necessary measures are in place for correcting and updating inaccurate data.

Storage limitation

You must not keep personal data for longer than you need it.

Integrity and confidentiality

You must implement adequate security controls to ensure that personal data is protected against loss, destruction or damage.

Accountability

You must have appropriate measures and records in place to be able to demonstrate your compliance.

03

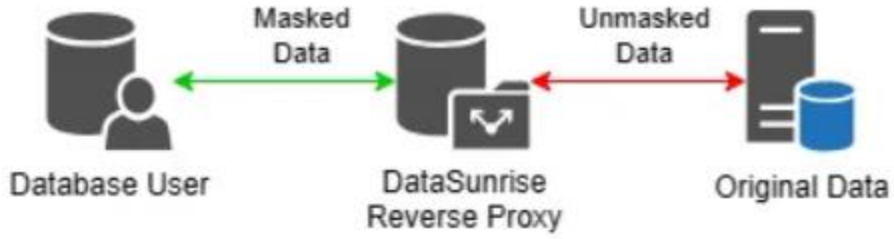
Data Privacy Technologies

Data Masking Techniques

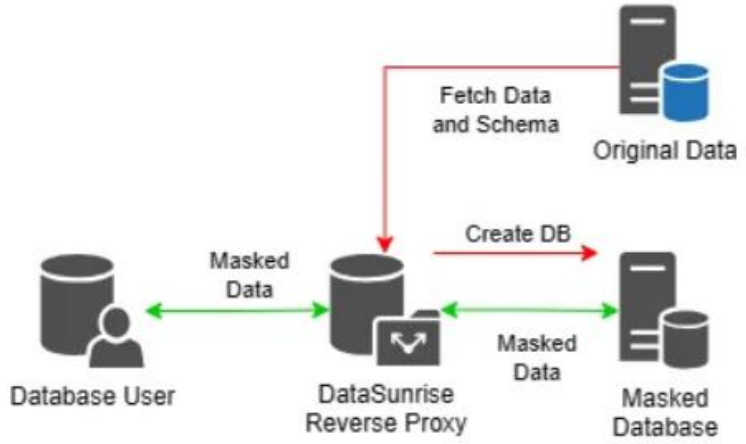
The process of hiding critical information in databases by replacing it with fictional characters or data.

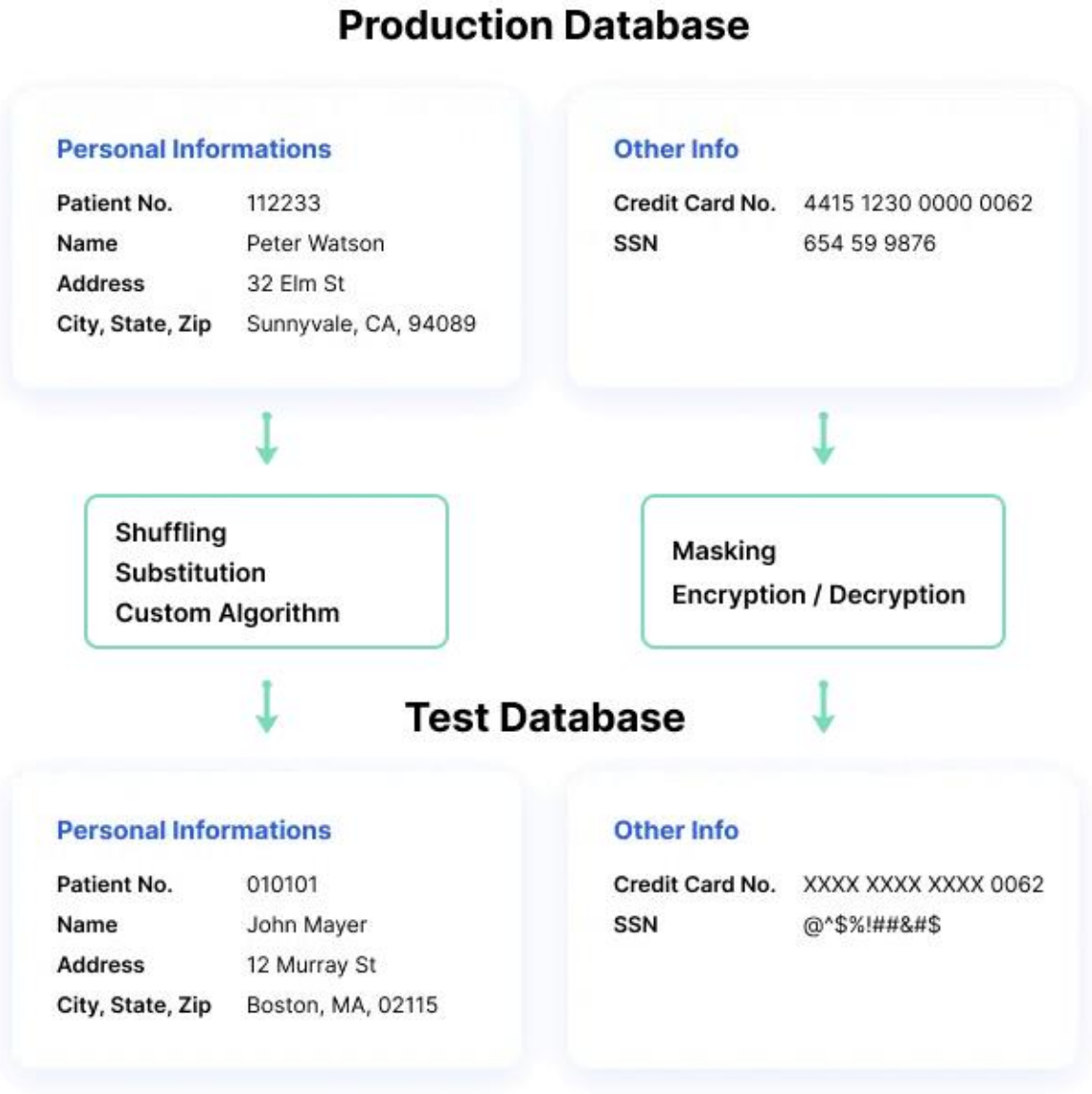
Anonymization and Pseudonymization

- **Dynamic Data Masking** happens on-the-fly, during data retrieval.



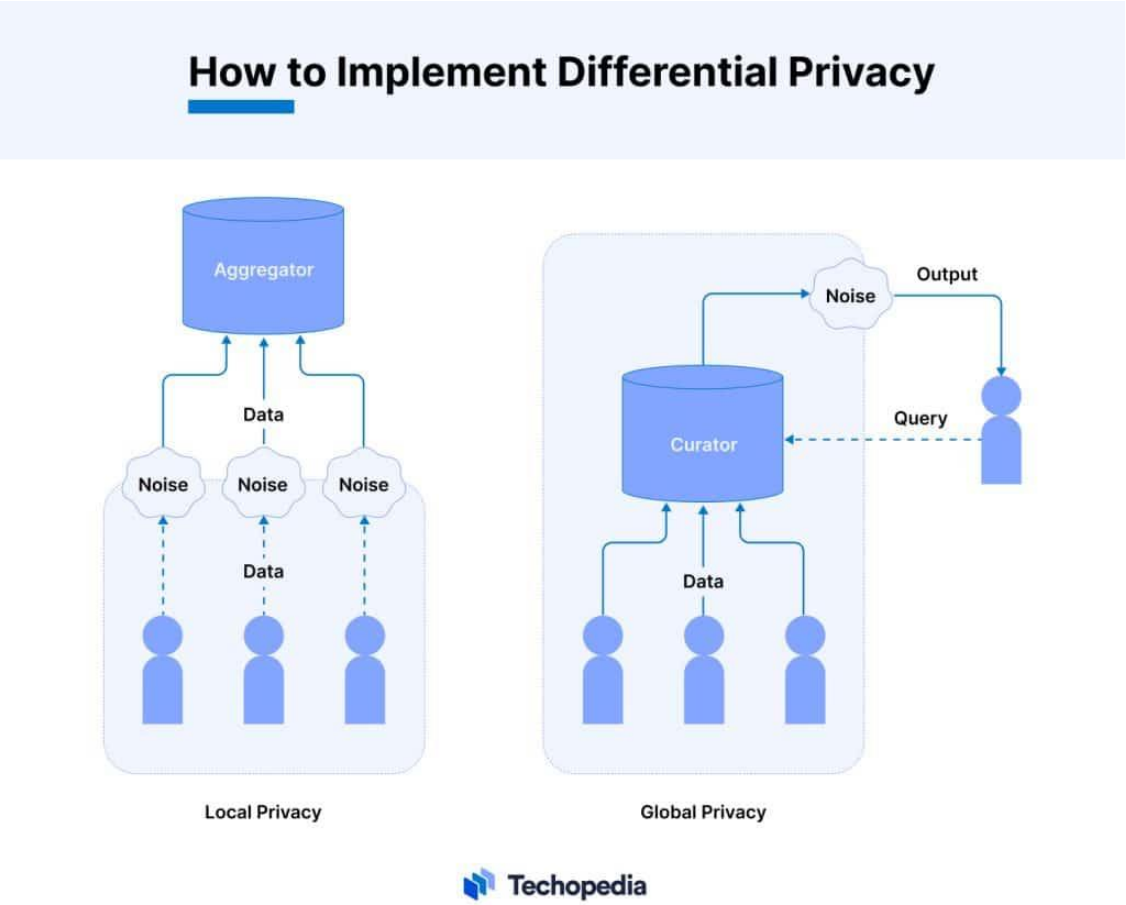
- **Static Data Masking** masks the data before moving it to a non-production environment.





Differential Privacy

A system for publicly sharing information about a dataset by describing the patterns of groups within the dataset while withholding information about individuals in the dataset.



Differential Privacy - Simply Explained - YouTube

Differential Privacy

Differential Privacy is a privacy-preserving technique aimed at ensuring that individual privacy is not exposed during data analysis or querying by adding noise to the data. Specifically, differential privacy ensures that any change to a single record in the dataset does not significantly impact the results of analysis, thus protecting the privacy of each individual. An algorithm has differential privacy if, for any two adjacent datasets (i.e., datasets differing by only one record), the output distribution of the algorithm does not change significantly. In other words, the query results from the algorithm do not allow determining whether a particular record exists in the dataset.

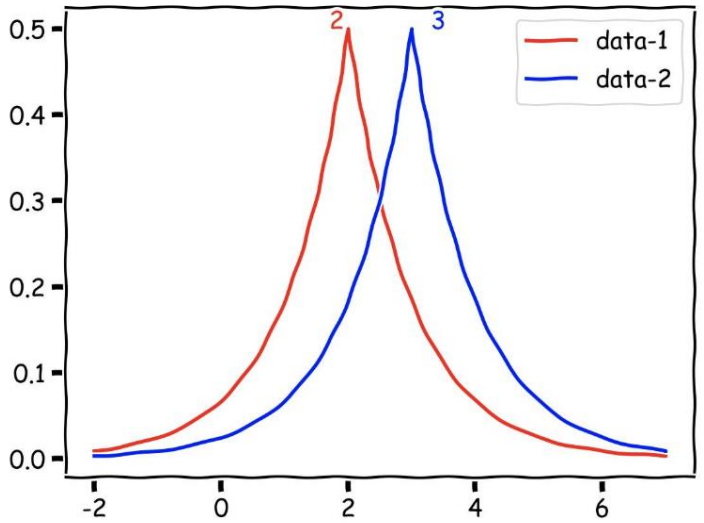
The core idea of differential privacy is to "blur" the data by adding noise (**such as Laplace or Gaussian noise)** to ensure that even if an attacker knows other data, the privacy of individual data records remains intact.

Anonymization and Pseudonymization

- **ε-Differential Privacy**: An algorithm satisfies ε-differential privacy if, for any two adjacent datasets D and D′, and any possible output S, the following condition holds:

$$\Pr[\mathrm{Alg}(D) \in S] \leq e^{\epsilon} \cdot \Pr[\mathrm{Alg}(D') \in S]$$

Here, ε (epsilon) is the privacy budget, indicating the level of privacy protection for the query results. The smaller the value of ε, the stronger the privacy protection.



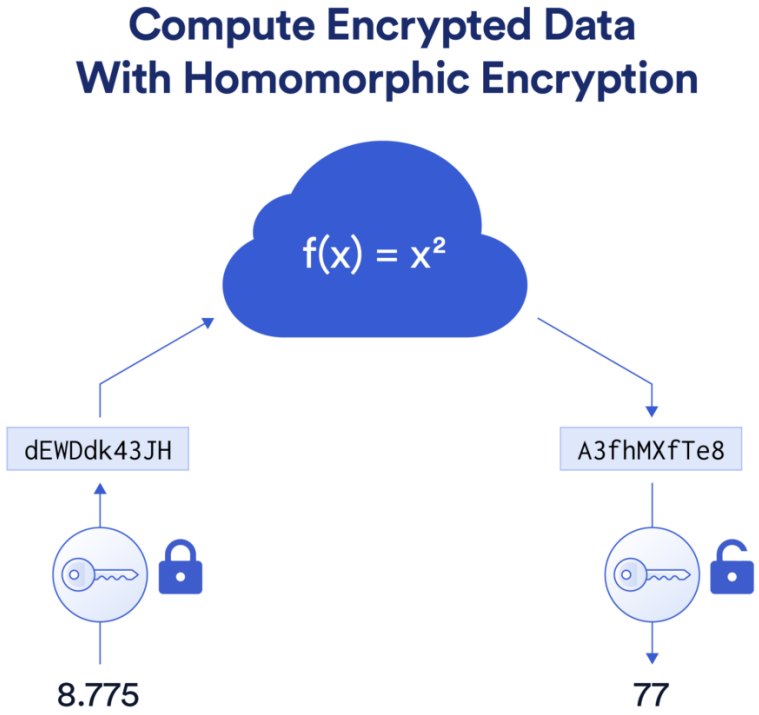
[1]The Algorithmic Foundations of Differential Privacy

Tokenization

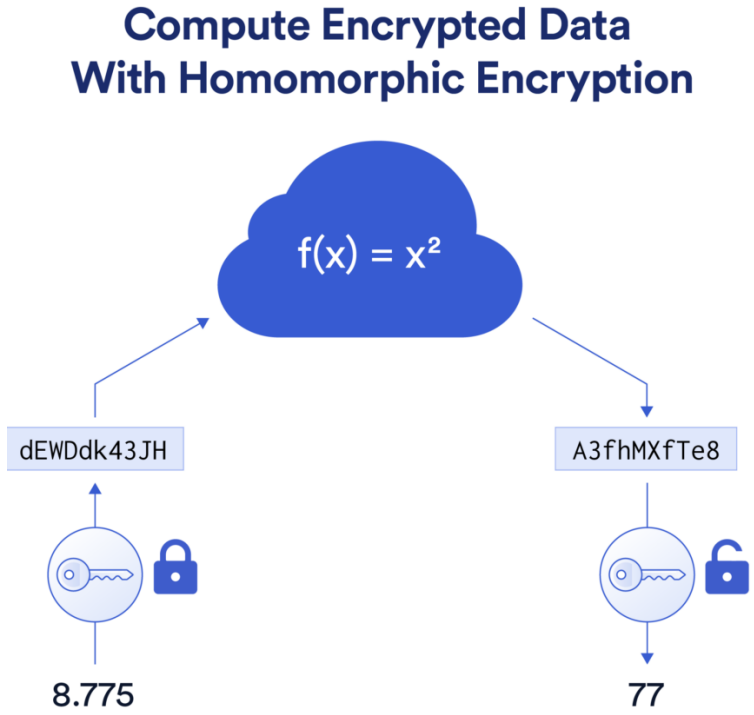
Tokenization is the process of replacing sensitive data with **non- sensitive equivalent identifiers**, known as tokens, which can be used in place of the original data without exposing it

Homomorphic Encryption

Homomorphic encryption (同态加密) is a form of encryption that allows for **computations to be carried out on ciphertext**, thus producing an encrypted result that, when decrypted, matches the result of operations performed on the plaintext.



Homomorphic Encryption



Example:

Suppose you have two numbers, `a = 5` and `b = 3`, and you want to compute their sum without directly exposing these numbers. You can use homomorphic encryption to encrypt them and then perform the addition on the encrypted data.

1. Encrypt `a` and `b`:

$$E(a) = \text{Encrypt}(a), \quad E(b) = \text{Encrypt}(b)$$

2. Then compute the sum of the encrypted values:

$$E(a+b) = \text{Encrypt}(a) + \text{Encrypt}(b)$$

3. Finally, decrypt the result to obtain the original computed result:

$$D(E(a+b)) = a+b$$

01.

Privacy Management Software.

Privacy management software is designed to help organizations comply with privacy regulations by automating the processes of data discovery, classification, and protection.

01. **Privacy Management Software.**

02. **Data Loss Prevention.**

Data loss prevention tools are designed to prevent data breaches by identifying, monitoring, and protecting sensitive data across networks, endpoints, and storage systems.

01. **Privacy Management Software.**

02. **Data Loss Prevention.**

03. **Privacy Impact Assessments.**

Privacy impact assessments are systematic processes used to identify and evaluate privacy risks associated with new projects or policies.

01. **Privacy Management Software.**

02. **Data Loss Prevention.**

03. **Privacy Impact Assessments.**

04. **Secure Messaging Apps.**

Secure messaging apps provide a platform for communication that prioritizes user privacy and data security.

04

Data Privacy Policies & Notices

Do you know any laws related to data privacy protection?

GDPR Compliance

GDPR Overview.

A comprehensive data protection regulation that applies to all organizations processing the personal data of individuals within the European Union.

GDPR Compliance

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU)

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

GDPR Overview.

A comprehensive data protection regulation that applies to all organizations processing the personal data of individuals within the European Union.

GDPR Requirements.

Clear consent for data processing

GDPR Compliance

GDPR Overview.

A comprehensive data protection regulation that applies to all organizations processing the personal data of individuals within the European Union.

GDPR Requirements.

Clear consent for data processing

GDPR Implementation.

- Conducting data protection impact assessments
- Updating privacy policies and notices
- Training staff on data protection responsibilities
- Implementing technical and organizational measures to secure personal data.

GDPR Compliance

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU)

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

GDPR Overview.

A comprehensive data protection regulation that applies to all organizations processing the personal data of individuals within the European Union.

GDPR Requirements.

Clear consent for data processing

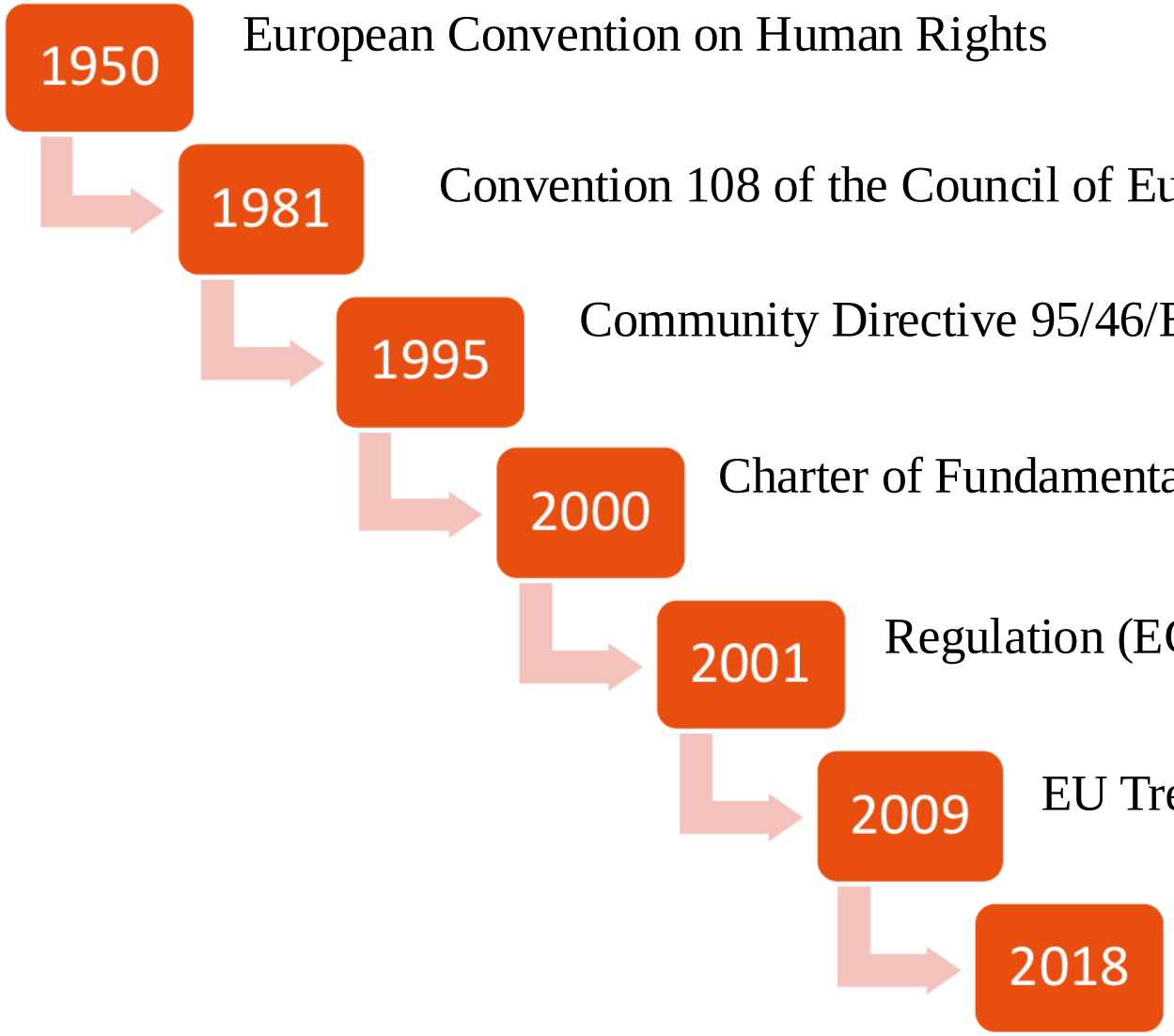
GDPR Implementation.

- Conducting data protection impact assessments
- Updating privacy policies and notices
- Training staff on data protection responsibilities
- Implementing technical and organizational measures to secure personal data.

GDPR Impact on Business.

Reevaluate their data processing practices and ensure compliance with the regulation

Legal Framework



GDPR in Numbers

190+
Countries potentially affected by the Regulation

28,000
Estimated number of new DPOs required in Europe

4%
of global turnover potential fines

80+
New requirements

7
Core data subjects rights

72
Hours given to report a data breach

Video Website: What are the 7 principles of GDPR?

AI knowledge Quiz

Which of the following is NOT one of the 7 principles of GDPR?

A. Security
B. Data Minimization
C. Data Sharing Priority
D. Accuracy

AI knowledge Quiz

Which GDPR principle requires data processing to align with the purpose of collection and not exceed the necessary scope?

A. Lawfulness, Fairness, and Transparency

B. Purpose Limitation

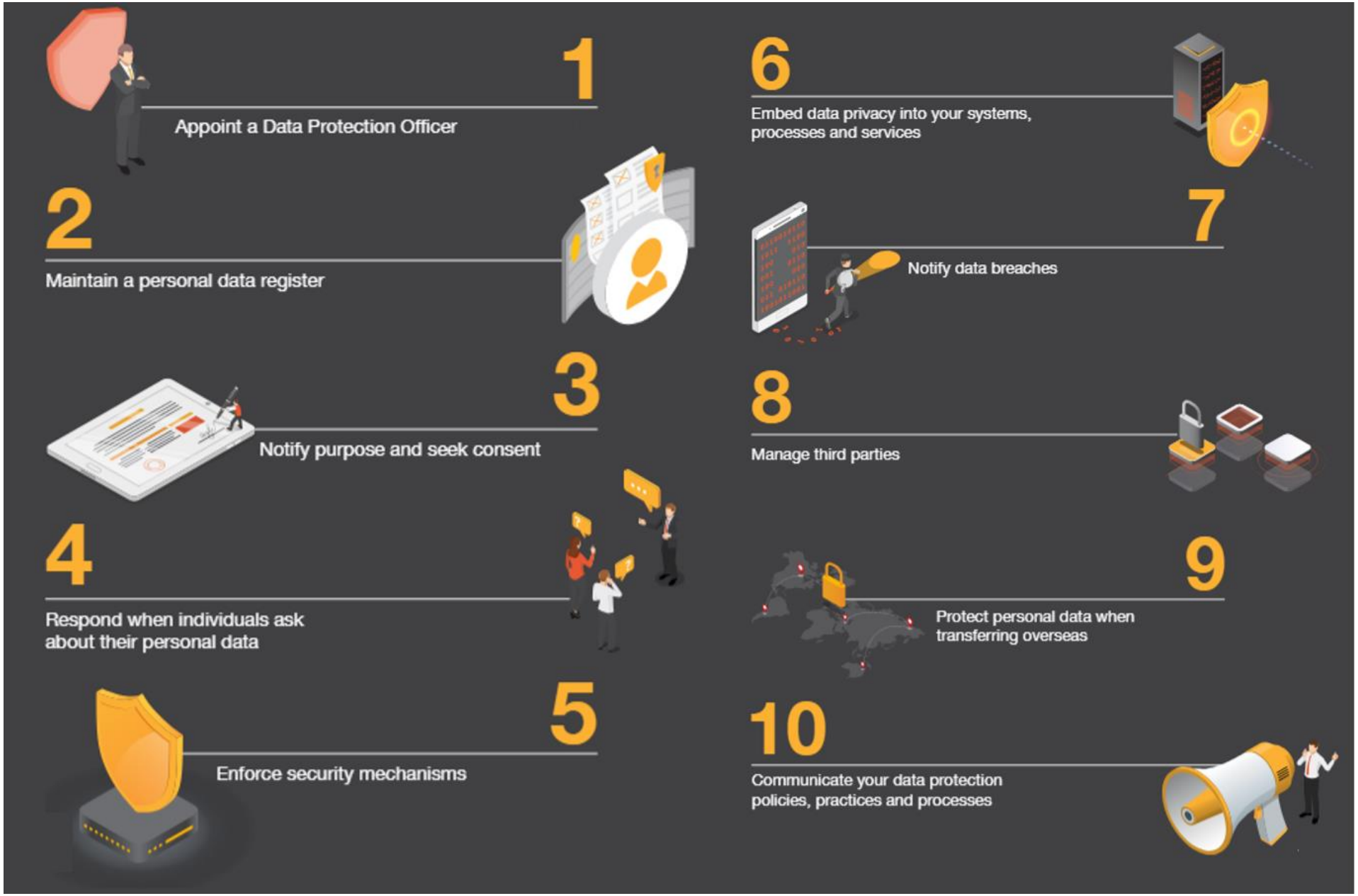
C. Data Minimization

D. Storage Limitation

05

Data Privacy in Practice

Ten steps to an effective data privacy programme



Appoint a Data Protection Office

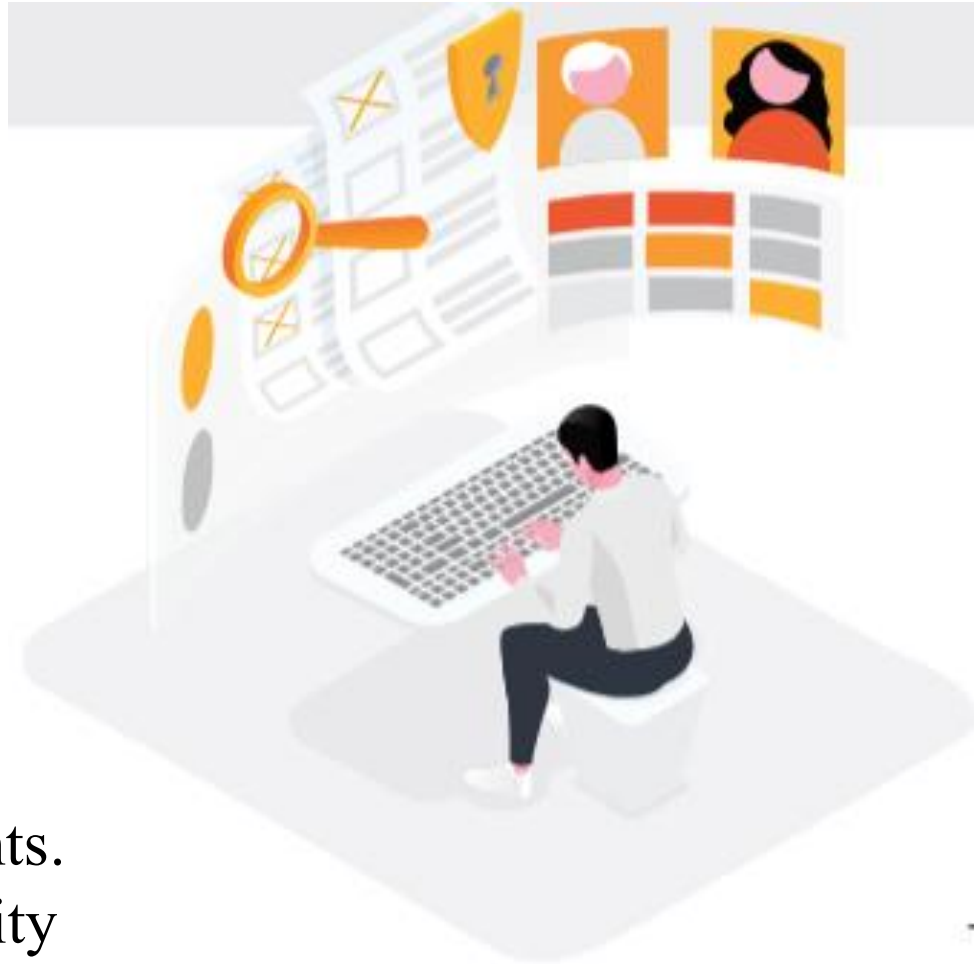
Many data privacy laws introduce the concept of **a 'Data Protection Officer' (DPO),** a new leadership role for overseeing the organisation's data protection

Maintain a personal data register

How can I identify personal data being processed?

Maintain a personal data register

What details should I include in the register?



- Name and contact details of your DPO and any other third party (if applicable).
- The lawful basis and purpose of processing the data.
- The different categories of personal data involved.
- The systems and locations where the personal data is processed.
- Where the data is transferred to and the list of recipients.
- The retention period and enforced technical and security measures

Notify purpose and seek consent

Transparency is a central principle in data privacy laws.

Notify purpose and seek consent

How can I obtain consent?

• Individuals can give their consent in writing or any other form. If the consent is given inwriting, it should be distinct from any otheragreement (e.g. terms and conditions) andwritten using clear and simple language.

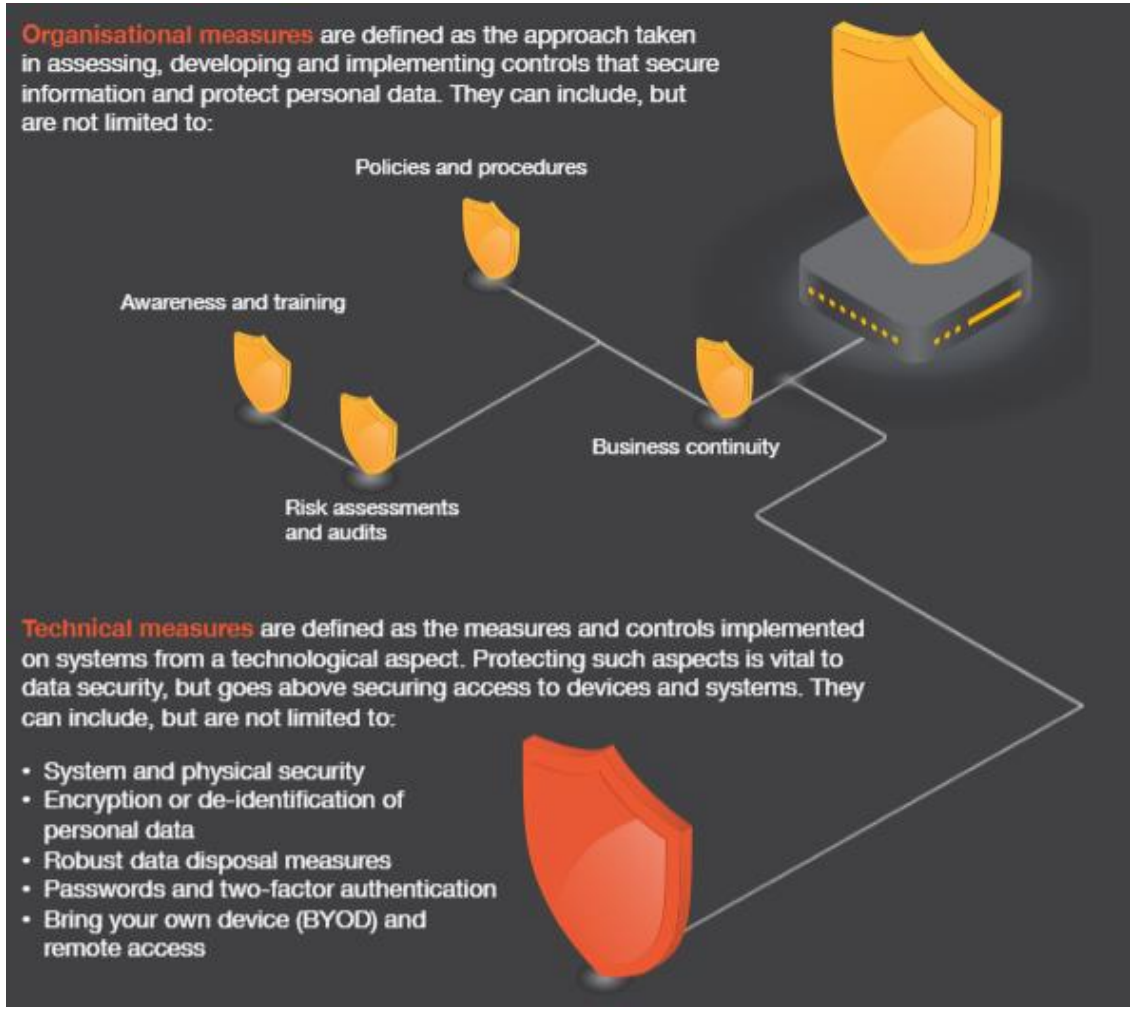
• Individuals can withdraw their consent atanytime, and the withdrawal proceduresshould be as easy as those for giving theconsent.

Respond when individuals ask about their personal data

- What are data subject requests?
- How can I be prepared?
- What information should I provide in my response?
- What are the steps to responding to a data subject request?

Enforce security mechanisms

Organisations needs to take reasonable steps to protect personal data.



Embed data privacy into your systems, processes and services

1. Privacy and data protection are embedded into the design of a new process or application.
2. Accountability is communicated and supported.
3. Transparency is created and maintained.
4. Safeguards are established and enabled.

Notify data breaches

How do I respond to a data breach?

- Assess the nature of the breach and confirm if personal data is involved.
- Identify what personal data has been impacted and how.
- Assess the impact of the breach to determine if it poses high risk to the rights and freedoms of individuals.
- Determine if you need to notify the Authority and the individuals concerned.
- Carry out a thorough investigation to identify the source of the breach.

Manage third parties

What should I include in a contract?

- The subject-matter and duration of processing
- The nature and purpose of processing
- The type of personal data and categories of data subjects
- The minimum terms or clauses required of the processor
- The obligations and rights of the controller

Protect personal data when transferring overseas

What is considered a third country data transfer?

- The personal data that you intend to transfer is in scope of one or more data privacy laws.
- The personal data is transferred to a third country.
- The receiver is a separate organisation or individual. This also covers transfers to anothercompany within the same corporate group.

Communicate your data protection policies, practices and processes

- Compliance with data privacy laws requires that **everybody** in the organisation understands their responsibilities to protect personal data.

- It is very important to communicate your data privacy policies and practices to your **customers and employees** to ensure they are familiar with how you process and protect personal data.

06

Future of Data Privacy

01

IoT Privacy

Emerging Privacy Issues

01 IoT Privacy

02 Facial Recognition

Emerging Privacy Issues

01 IoT Privacy

02 Facial Recognition

03 Deepfakes

Emerging Privacy Issues

https://www.youtube.com/watch?v=2k08H4MRJoQ

Emerging Privacy Issues

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU)

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

01 IoT Privacy

02 Facial Recognition

03 Deepfakes

04 Quantum Computing

Propose New Privacy Regulations:

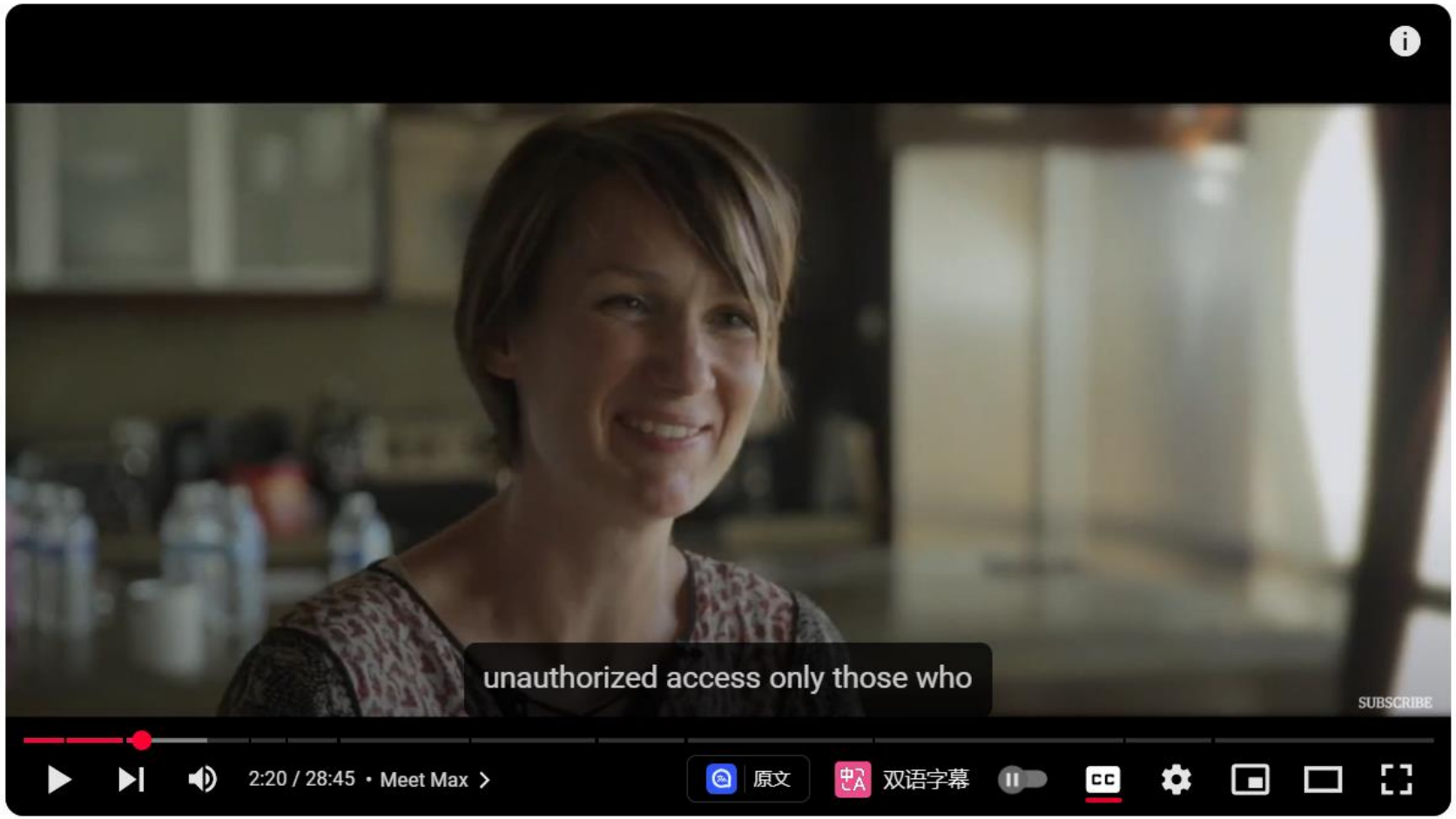
- Suggest new or modified privacy regulations to **address current data security concerns**. Regulations should aim to protect user privacy without impeding technological innovation.
- Use AI tools like ChatGPT or Deepseek to brainstorm ideas, analyze privacy risks, or refine your proposed regulations.
- Upload your proposal **on Canvas (10 minutes).**
- Anyone who actively shares their AI insights with the class will earn a small bonus reward.
- **Practice is not included in the final score.**

The Power of Privacy – documentary film

If you are interested, you can watch this documentary after class.

In this film, Aleks Krotoski travels the world to undergo challenges that explore our digital life in the 21st century. Watch her be stalked and hacked, fight to get leaked documents back, dive into open data and live in a futuristic home that monitors her every move.

Video Website: https://www.youtube.com/watch?v=KGX-c5BJNFk



THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU)

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

AIAA 2290: Ethics, Privacy and Security in AI

Thank you

Xuming HU

xuminghu@hkust-gz.edu.cn

The Hong Kong University of Science and Technology (Guangzhou)

2025 Spring