**1.**

**What is Data?**

Data, Data refers to information represented in the form of numbers, text, images, or sound. It is an indispensable part of modern society and the foundation of information. Data itself has no intrinsic value, but after processing and analysis, valuable information and insights can be extracted. The data types are mainly divided into quantitative data and qualitative data. Quantitative data is represented by numbers and can be subjected to arithmetic operations, such as age, weight, etc; Qualitative data, on the other hand, is represented using non numeric representations to describe the characteristics or categories of the object, such as gender, occupation, etc.

**What is Information?**

Information, Information is processed, organised and interpreted data that has some meaning and value to the receiver. It is a property of things that represents the meaning or context of data. Information is something we can link to data in order to give it meaning. Unlike data, information is valuable because it provides understanding, knowledge, or meaning about things. For example, the number "36" is data, but when we know that "36" represents someone's age, it becomes information.

**What is the difference between Data and Information?**

The main difference between data and information lies in their meaning and value. Data is the original form of information, a collection of symbols that have not been interpreted or given meaning. And information is the result of data being processed, interpreted, and given meaning. In short, data is a record of facts or observations, while information is the meaning or content represented by these data.

**What is Metadata?**

Metadata, Metadata refers to the data about data that describes data. It mainly describes the attribute information of data, such as the source, format, size, creation time, modification time, etc. Metadata is used to support the storage, retrieval, management, and utilization of data. Through metadata, we can better understand and utilize data resources.

**Why we need metadata?** The main reasons why we need metadata are as follows:

1)Data management and organization: Metadata helps to effectively manage and organize data, making it easier for users to find and access the data resources they need.

2)Data retrieval: Through metadata, it is possible to quickly retrieve datasets that meet specific conditions, improving the efficiency of data utilization.

3)Data sharing and exchange: In the process of data sharing and exchange, metadata can ensure the consistency and accuracy of data, reducing misunderstandings and errors.

4)Data security and privacy protection: Metadata can also be used to develop data security and privacy protection policies, ensuring the legitimate use of data and protecting personal privacy.

**2.**

**Data Privacy**

Data privacy refers to the state in which personal information is protected during the collection, storage, transmission, and use process. It focuses on how to ensure that personal data is not accessed, used, disclosed or leaked without authorization, in order to safeguard personal privacy rights.

**Key Elements of Data Privacy Compliance**

1)Practices: e.g. data encryption, access control, user authorisation, etc.

2)Rules: laws and regulations (e.g., GDPR, etc.), industry norms, and privacy policies developed internally by companies.

3)Guidelines: guidelines issued by regulators on data privacy protection.

4)Tools: e.g. Privacy Enhancing Technologies (PETs), including anonymisation tools, encryption software, etc.

**For Individuals:**

Protecting personal privacy: Data privacy protection ensures that individuals' private information is not accessed or used without authorization, safeguarding their privacy rights.

Preventing identity theft and fraud: Strong data privacy protection measures can reduce the risk of identity theft and fraud, protecting individuals' property and reputation.

Enhancing trust: When personal data is properly protected, individuals are more willing to share information, thereby promoting the healthy development of the digital economy.

**For Businesses:**

Compliance with laws and regulations: Protecting user data privacy is a fundamental requirement for enterprises to comply with laws and regulations, avoiding fines and reputation damage caused by illegal activities.

Maintaining user trust: Protecting user data privacy can enhance users' trust in the enterprise, improve brand image, and increase user loyalty.

Promoting business development: Reasonable use of user data can bring commercial value to enterprises, but the prerequisite is to ensure the legality and privacy of the data.

**Differences and Concerns**

**Differences:**

**Focus:** Individuals are more concerned about the protection of personal privacy and preventing the abuse of personal information; And enterprises need to use data reasonably to promote business development while protecting user privacy.

Scope of responsibility: Individuals are the direct owners of data and bear ultimate responsibility for the protection of personal data; As data collectors and processors, enterprises need to bear more legal and technical responsibilities.

**Concerns:**

1)Individual: Worried about personal data being illegally collected, stored, used, and leaked, leading to risks such as privacy breaches and identity theft.

2)Enterprises: They are concerned about the legal risks and reputational damage they may face due to data breaches or misuse, while balancing the relationship between data usage and user privacy protection.

In summary, data privacy protection is crucial for both individuals and businesses. Individuals need to pay attention to the protection of personal privacy, while enterprises need to use data reasonably to promote business development on the basis of complying with laws and regulations, while ensuring the privacy and security of user data.

**3.**

**Possible security threats to databases**

1)Malicious network attacks: e.g. SQL injection attacks, Denial of Service (DoS) attacks, etc.

2)Software Vulnerabilities: Possible vulnerabilities in the database software itself that can be exploited by attackers.

3)Intrusion: Unauthorised access to the database system.

4)Misuse: Improper use by internal personnel, such as deleting data by mistake.

5)Negligence and Damage: Data loss or damage caused by e.g. hardware failure, natural disasters, etc.

**Database Security Measures**

1)Tools: Use encryption tools to encrypt data, such as symmetric encryption and asymmetric encryption; use firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to prevent external attacks.

2)Processes: Establish data backup and recovery processes to cope with data loss; develop strict user access control processes, including user authentication, authorisation and auditing.

3)Methodology: Adopt secure development methodology and incorporate security awareness into the database development process, such as secure coding specification and vulnerability scanning.