BT:

Task2. 1. Data refers to raw facts and figures. It can be numbers, characters, symbols, or even images, sounds, etc. For example, a list of numbers such as 1, 2, 3, 4, 5 is data. In a database of a store, the product codes, prices, and inventory quantities are all forms of data. Data on its own doesn't have much meaning. It's just a collection of values.

2. Information is data that has been processed, organized, or structured in a way that is meaningful and useful. For example, if you have a list of daily temperatures (data), and you calculate the average temperature for a month and present it in a graph with labels showing the months and years, that becomes information. Information provides context and understanding that helps in decision - making. For a business, sales data (number of units sold of different products, prices, etc.) can be analyzed to provide information such as which products are the best - sellers, which regions have the highest sales, and how sales are trending over time.

3. Difference between Data and Information

Nature: Data is the raw material. It's like the individual bricks. For example, a set of students' test scores without any analysis is data. Information is the end - product that is derived from data. It's like a building made out of those bricks. Using the students' test scores, you can calculate the average score, the highest and lowest scores, and the percentage of students who passed. This analyzed result is information.

Usefulness: Data on its own may not be directly useful for decision - making. For example, a long list of customer ID numbers doesn't tell you much about your customers' behavior.

Information is actionable. If you know that a particular product has had a 50% increase in sales over the last quarter (information), you can make decisions such as increasing production or running a marketing campaign to further boost sales.

4. Metadata is data about data. It provides information about the characteristics, context, and quality of the data. For example, in a digital photo, metadata might include the date and time the photo was taken, the camera model used, the resolution of the photo, and the location (if the camera has GPS). In a database, metadata can include information such as the data type of a field (e.g., integer, text), the length of a field, and the relationships between different tables.

5. Why we need Metadata?

Data Management and Organization: It helps in efficient storage and retrieval of data. For example, in a large library of digital documents, metadata about the author, topic, and publication date can be used to quickly find relevant documents.

Data Quality and Integrity: Metadata can indicate the source and accuracy of data. If you know that a particular dataset was collected through a reliable survey method (metadata about data collection), you can have more confidence in using that data.

Interoperability: When different systems need to share and understand data, metadata provides a common language. For example, in a healthcare setting, metadata about patient records (such as the format of medical codes) allows different hospitals and clinics to exchange and make sense of patient data.

MT:

Task3. 1. Data privacy refers to the protection of personal data from unauthorized access, use, disclosure, and destruction. It is about ensuring that individuals have control over their own personal information and that organizations handle such data in a legal and ethical manner.

2. **Practices:**

Data Minimization: Organizations should only collect and store the data that is necessary for a specific purpose. For example, an e - commerce company should only collect the customer's shipping address if it's relevant to the order fulfillment process.

Access Control: Limit access to personal data to only those employees who need it for their job functions. For instance, in a hospital, only the medical staff directly involved in a patient's treatment should have access to the patient's full medical records. This can be implemented through user authentication and authorization systems such as passwords, multi - factor authentication, and role - based access control.

Data Encryption: Encrypting sensitive data both at rest (when it's stored in databases or on servers) and in transit (when it's being transferred over networks). For example, financial institutions encrypt customers' banking details during online transactions to prevent interception and unauthorized access.

Rules and Guidelines:

Compliance with Regulations: Adhere to laws such as the General Data Protection Regulation (GDPR) in the European Union or the California Consumer Privacy Act (CCPA). These regulations stipulate requirements such as obtaining consent from individuals before collecting their data, providing individuals with the right to access and delete their data, and notifying them in case of a data breach.

Privacy Policies: Have clear and comprehensive privacy policies that are easily accessible to customers and users. The policy should explain what data is collected, how it's used, with

whom it's shared, and how it's protected. For example, a social media platform's privacy policy should detail how user - generated content, such as photos and posts, are used for advertising or other purposes.

Tools:

Data Loss Prevention (DLP) Tools: These tools monitor and prevent the unauthorized transfer of sensitive data. For example, they can detect and block an employee from sending a file containing customer credit card numbers to an external, unauthorized email address.

Privacy Impact Assessment (PIA) Tools: Used to evaluate the potential privacy risks associated with a new project, system, or process. For example, before launching a new mobile app that collects user location data, a company can use a PIA tool to identify and mitigate any privacy risks.

3.**For Individuals**

Personal Autonomy: Data privacy is crucial for maintaining an individual's autonomy over their personal lives. Personal information such as financial details, health records, and social relationships can be misused if not protected. For example, if a person's credit card details are stolen due to a data breach, it can lead to unauthorized transactions and financial losses.

Reputation and Trust: Protecting personal data helps in safeguarding an individual's reputation. For example, if a person's private photos or messages are leaked without their consent, it can cause emotional distress and damage to their social and personal life.

For Businesses

Customer Trust: Maintaining data privacy builds customer trust. Customers are more likely to do business with companies that they believe will protect their personal information. For example, a bank that has a strong reputation for data security is more likely to attract and retain customers.

Legal and Regulatory Compliance: Non - compliance with data privacy laws can lead to severe financial penalties. For example, under the GDPR, companies can be fined up to 4% of their global annual turnover for serious violations.

Business Reputation: A data privacy breach can damage a company's reputation, leading to a loss of customers and business partners. For example, if a major retailer experiences a data breach that exposes customer credit card information, it can lead to a significant drop in sales and a damaged brand image.