1. People use spoken commands to interact with digital assistants.

   Explain **one** ethical concern associated with digital assistant technologies.

   (2)

2. Consent must be obtained before organisations can use personal data.

   Give **two** pieces of information that organisations must tell people when requesting consent to use their personal data.

   (2)

3. Data protection legislation sets out principles that organisations must follow.

   Give **two** of these principles.

   (2)

4. Which of the following rights does the Data Protection Act 2018 provide to individuals regarding their personal data? (1)

   a) The right to be forgotten b) The right to access personal data
   c) The right to edit inaccurate personal data d) All of the above

5. Give 2 ways that organizations can ensure that they handle personal data in compliance with data protection laws? (2)

6. Explain the concept of informed consent in the context of data collection. (2)

7. A travel company supports international travellers.

   Discuss the legal and ethical issues associated with the company's collection and use of data.

   Your answer should consider:

   - the principles of the Data Protection Act
   - The rights of the customers
   - the responsibilities of the travel company.
   - You could consider privacy (the necessity of it, how invasive asking for it is, security of the collected data, discrimination (data might be misused), transparency (is the company being transparent about what they are collecting and how they are storing and using it), consent

   (6)

ANSWERS

1. Here are the ethical concerns surrounding the use of digital assistants. Many of these points can be applied to other scenarios.
   Lack of Transparency:
   Users may not fully understand how their data is being used or how the assistant arrived at a particular response.

   Data Security and Usage: Digital assistants are constantly collecting user data through voice commands, interactions, and even recordings depending on settings. This data can include personal details, conversations, and even background noises, raising concerns about user privacy. The security of this collected data is crucial. Breaches or unauthorized access could expose sensitive information. Additionally, the way companies use this data for targeted advertising or other purposes needs clear user consent and transparency.
   Algorithmic bias and discrimination:
   Digital assistants rely on algorithms trained on massive datasets that might reflect biases in society. This can lead to discriminatory outcomes in areas like search results, news recommendations, or even how the assistant interacts with users based on their speech patterns.
   Limited Accessibility: Digital assistants primarily rely on voice commands, potentially excluding people with disabilities or those who don't speak the dominant language fluently.
   Echo Chambers: Digital assistants can personalise information based on user behaviour, potentially creating echo chambers where users are only exposed to information that confirms their existing beliefs.

2. **Under UK GDPR,** there are a number of pieces of information that organisations should tell us when collecting data.
   The specific purposes for which the data will be used: This means organizations must clearly explain what they will be doing with the data they collect. For example, they might need consent to use your data for:
   - Sending you marketing communications
   - Sharing your data with third parties
   - Creating a user profile for personalised services

   Being specific allows users to understand how their data will be used and make informed choices about whether to consent.
   Their right to withdraw consent at any time: Organisations must inform individuals that they have the right to withdraw their consent for data processing at any time. This allows users to control their data and lets them change their mind about how their information is used.
   The retention period for the data: Organisations should inform you about how long they intend to keep your personal data.

3. **Here are the main principles of UK GDPR (General Data Protection Regulations):**
   - Data must be processed lawfully
   - Purpose limitation – can only be used for the purpose stated
   - Data minimisation – only collect the minimum data needed for the purpose
   - Accuracy – data must be accurate and kept up to date
   - Storage limitation – data can only be kept for a certain period of time
   - Stored securely – must be kept secure and safe
   - Accountability – the organisation must be responsible for enforcing the GDPR

   In addition there are further rights for the users:
   Right to access: Users have the right to request a copy of their data from the organization.
   Right to rectification: Users have the right to request correction of any inaccurate information held about them.

Right to erasure (right to be forgotten): In certain situations, users can request deletion of their personal data.
Right to restrict processing: Users can request limitations on how their data is processed.
Right to data portability: Users can request their data to be transferred to another organisation
Right to object: Users have the right to object to automated decision-making based on their data.
Right to withdraw consent: Users have the right to withdraw their consent for data processing at any time.

4. D – all of the above

5. Organisations should have a Data Controller who is in charge of making sure that GDPR is followed. There should be a clear **Privacy Policy** outlining what data is collected, how it's used, and with whom it's shared. **Meaningful Consent**: Obtain explicit and informed consent from users for data collection and use. Avoid pre-checked boxes or confusing language. **Data Security**: Maintain robust security measures to protect personal data from unauthorised access.

6. Informed consent ensures individuals **understand how** their personal data is being collected and used before they agree to it. Pre-checked boxes or misleading language shouldn't be used to obtain consent. Users should have a **clear way to opt-out** or withdraw consent at any time. **Understanding**: Individuals should understand the potential consequences of giving consent. This might include understanding how their data might be used for targeted advertising or shared with third parties.

7. Longer answer question – here are some points that you could have made

Benefits of Data Collection for Travel Companies (could be applied to other industries)

Personalisation: Explain how data can be used to personalise travel recommendations, deals, and marketing messages for each customer.

Improved Customer Experience: Describe how data can be used to streamline booking processes, offer targeted travel assistance, and enhance overall customer satisfaction.

Business Insights: Explain how data can be used to understand customer preferences, travel trends, and optimise marketing strategies.

Ethical Concerns with Data Collection

Privacy Intrusion: Discuss concerns about the extent of data collection, including personal details, travel history, and browsing behaviour.

Data Security Risks: Highlight the potential for data breaches and unauthorised access to sensitive customer information.

Profiling and Targeting: Discuss ethical concerns around creating customer profiles and using them for targeted advertising or potentially discriminatory practices.

Legal Issues with Data Collection

International Data Transfer: Explore the legal challenges associated with transferring customer data across international borders with different data protection regulations.

Consent and Transparency: Discuss the importance of obtaining informed consent from customers for data collection and ensuring clear communication about data usage.

Compliance with Data Protection Laws: Explain the need for travel companies to comply with relevant data protection laws, such as the UK GDPR.

Minimising Risks and Ensuring Ethical Practices

Data Minimisation: Discuss the importance of collecting only the data necessary for specific purposes and avoiding unnecessary data collection.

Strong Security Measures: Highlight the need for robust security measures to protect customer data from breaches and unauthorised access.

Transparency and User Control: Explain the importance of clear privacy policies, providing options for users to control their data, and the right to withdraw consent.