Question 2

28 marks

A smart home system features an AI assistant that monitors household activities, learns routines, and controls interconnected devices (e.g., lights, thermostats, security cameras). It collects continuous data on occupant presence, energy consumption, and environmental conditions. The company's servers are located overseas, and it occasionally employs third-party contractors for system maintenance and data analysis.

a) Explain the importance of transparency for users regarding the data practices of this smart home system. Identify two Australian Privacy Principles that would guide the system's management of personal information and describe how the company should implement these principles.
(10 marks)

b) Analyse the specific privacy challenges that arise when a smart home system stores and processes user data overseas and uses third-party contractors. Identify one Australian Privacy Principle that directly addresses cross-border data management and explain the responsibilities of the company. (9 marks)

c) Discuss the necessity of maintaining quality (accuracy, completeness, and up-to-dateness) of the collected data. Identify one Australian Privacy Principle related to data quality and another related to individual access to personal information, and explain how these principles empower users in managing their data within this system. (9 marks)

Marking Guide

Part A

Marks	Criteria	Evidence of achievement
1	Defines transparency	States transparency means informing users clearly about data collection and use.
1	Explains importance	Notes transparency builds user trust and accountability in the system.
1	Identifies APP 1 (Open and transparent management)	States organisations must manage data practices openly.
1	Explains APP 1	Requires a clear, up-to-date privacy policy about how data is collected and handled.
1	Implementation of APP 1	Example: publish accessible privacy statements and provide updates when practices change.
1	Identifies APP 5 (Notification of collection)	States users must be notified when and why personal data is collected.
1	Explains APP 5	Requires disclosure of purposes, retention, and possible sharing of data.
1	Implementation of APP 5	Example: notifications on initial setup and within the AI assistant's app dashboard.
1	Links transparency to user control	Explains transparency enables informed decisions about participation.
1	Integrates APPs with ethical obligation	Connects principles to fairness, consent, and safeguarding household privacy.

Sample Response

Transparency means making sure users clearly understand what data is being collected, why it is collected, and how it will be used or shared. In a smart home system where the AI assistant constantly monitors occupant behaviour, transparency is essential for trust and ethical data use. Without it, users cannot give meaningful consent.

APP 1 (Open and transparent management of personal information) requires organisations to have an up-to-date, accessible privacy policy that describes data practices. The company should implement this by publishing a clear privacy statement on its website and app, outlining what personal information (e.g. energy use, presence, security footage) is collected, how it is processed, and how long it is stored.

APP 5 (Notification of the collection of personal information) requires users to be informed when personal information is collected and why. The company should provide this notice during device setup and through ongoing app notifications, so users know what data is being gathered and if it is shared with contractors. Together, APP 1 and APP 5 ensure data practices are open and understandable.

Part B

Marks	Criteria	Evidence of achievement
1	Identifies overseas storage as challenge	States data stored abroad increases risks to privacy.
1	Explains risk of different legal systems	Notes foreign jurisdictions may have weaker privacy protections.
1	Identifies third-party contractor risk	Contractors may access data without strong safeguards.
1	Identifies APP 8 (Cross-border disclosure)	States APP 8 governs sending personal information overseas.
1	Explains APP 8 responsibility	Notes company must ensure overseas recipients comply with APP standards.
1	Implementation: due diligence	Example: contractual agreements requiring APP-equivalent protection.
1	Implementation: technical safeguards	Example: encrypted transfers and access logging for overseas servers.
1	Links APP 8 to accountability	Company remains responsible even if data handled by third parties.
1	Integrates analysis with smart home context	Explains overseas storage and contractors must be strictly managed to protect households.

Sample Response

Storing data on overseas servers and using third-party contractors creates specific privacy risks. Different jurisdictions may not provide the same level of protection, and contractors could mishandle or expose data. Users' household routines, security camera feeds, and presence information are highly sensitive and must remain safeguarded.

APP 8 (Cross-border disclosure of personal information) states that if data is sent overseas, the company must ensure the recipient upholds protections comparable to Australian law. The company remains responsible for the data, even when handled abroad.

To comply, the company should conduct due diligence by requiring binding contractual agreements with overseas providers and contractors to meet APP standards. Technical safeguards should include encrypted transfers, access controls, and regular audits. This ensures accountability and prevents misuse of data while enabling the benefits of overseas infrastructure.

Part C

Marks	Criteria	Evidence of achievement
1	Explains importance of data quality	States accuracy, completeness, and currency of data are critical for reliable service.
1	Identifies risk of poor-quality data	Notes incorrect data may cause wrong device actions or energy inefficiencies.
1	Identifies APP 10 (Quality of personal information)	States APP 10 requires organisations to keep data accurate, complete, up-to-date.
1	Explains APP 10 in context	Example: system must regularly update occupancy and energy data.
1	Identifies APP 12 (Access to personal information)	States APP 12 gives individuals the right to access their own data.
1	Explains APP 12 in context	Example: users must be able to view data collected via dashboards or reports.
1	Explains empowerment through quality	Notes data accuracy ensures fair treatment and trustworthy AI decisions.
1	Explains empowerment through access	States access enables users to challenge errors and request corrections.
1	Integrates APPs and ethics	Concludes these principles ensure fairness, accuracy, and user control of personal data.

Sample Response

The reliability of the smart home system depends on the quality of data. If occupancy data is incomplete or outdated, devices may act incorrectly, such as lights turning off while people are home or thermostats mismanaging temperature. High-quality data improves efficiency, safety, and user trust.

APP 10 (Quality of personal information) requires organisations to take reasonable steps to ensure personal data is accurate, complete, and up-to-date. The company should regularly refresh sensor readings, synchronise data from wearables, and allow users to update their personal preferences.

APP 12 (Access to personal information) gives individuals the right to access their own data. In this context, users should be able to log into the system dashboard to see energy consumption records, activity logs, and environmental data. They should also be able to request corrections if errors are found.

Together, these principles empower users by ensuring the data guiding the AI is trustworthy and by giving them control to review and correct what is collected. This safeguards fairness and accountability in the platform's operation.