The **Australian Privacy Principles (APPs)** under the **Privacy Act 1988** provide a framework for how personal information must be managed by organisations and agencies in Australia. These principles ensure that personal information is collected, stored, used, and disclosed responsibly, and protect individuals' privacy.

Overview of the 13 APPs

1. Open and Transparent Management of Personal Information

- Organisations must have a clear and up-to-date privacy policy detailing how personal information is managed.
- The privacy policy should include details about how individuals can access their information and lodge complaints.

2. Anonymity and Pseudonymity

- Where lawful and practicable, individuals must be given the option to interact anonymously or use a pseudonym.

3. Collection of Solicited Personal Information

- Personal information must only be collected if it is necessary for the organisation's activities or functions.
- Information must be collected lawfully and fairly.

4. Dealing with Unsolicited Personal Information

- If an organisation receives unsolicited personal information, it must assess whether it could have been collected lawfully.
- If not, the information must be destroyed or de-identified.

5. Notification of the Collection of Personal Information

- Individuals must be informed about the collection of their personal information, including:
    - The purpose of collection.
    - How the information will be used and disclosed.
    - Their rights to access and correct the information.

6. Use or Disclosure of Personal Information

- Personal information must only be used or disclosed for the primary purpose for which it was collected, unless:
    - The individual consents to another use.
    - There is a legal obligation to disclose it.

7. Direct Marketing

- Personal information must not be used for direct marketing without the individual’s consent.

- Individuals must have a way to opt-out of marketing communications.

8. Cross-Border Disclosure of Personal Information

- Organisations must ensure that personal information disclosed to overseas recipients is protected at a level comparable to the APPs.
- Individuals must be informed if their information is sent overseas.

9. Adoption, Use, or Disclosure of Government-Related Identifiers

- Government-issued identifiers (e.g., Medicare numbers) must not be used as an organisation's own identifier unless permitted by law.

10. Quality of Personal Information

- Organisations must take reasonable steps to ensure the personal information they collect, use, or disclose is accurate, complete, and up to date.

11. Security of Personal Information

- Personal information must be protected against misuse, loss, unauthorized access, modification, or disclosure.
- When no longer needed, information must be securely destroyed or de-identified.

12. Access to Personal Information

- Individuals have the right to access their personal information held by an organisation.
- Access may only be refused in specific circumstances (e.g., if it impacts another person's privacy).

13. Correction of Personal Information

- Organisations must take reasonable steps to correct personal information if it is inaccurate, incomplete, out-of-date, or misleading.
- Individuals must be informed of their rights to request corrections.

Applicability of APPs

- The APPs apply to Australian Government agencies and private organisations with an annual turnover of $3 million or more, as well as certain smaller organisations such as health service providers.

Importance in the NDIS Context

The APPs are particularly important in the context of the NDIS to ensure that participants' sensitive information is handled with the utmost care, providing transparency, security, and rights to individuals. Compliance with these principles fosters trust and ensures ethical data management practices.