Ten Principles of Personal Information Protection

The *Personal Information and Protection Act* (PIPA) is based on ten principles of personal information protection. These principles explain the intent of the Act.

They are:

1. Accountability

- Each organization must appoint an individual, or individuals, responsible for ensuring compliance with PIPA.
- An organization is responsible for the personal information under its control. It must implement policies and practices that apply these principles.

2. Identifying purposes

- Organizations must identify how they will use information when they collect it.
- Organizations must tell individuals why they are collecting personal information.
- If an organization wants to use information in a different way at a later date, it must get the individual's consent.

3. Consent

- Individuals must know about, and consent to, the collection of personal information about them.
- The supply of a product or service may not be made conditional on consent to the collection of non-essential information.

4. Limiting collection

- Organizations may only collect the information that is necessary for the identified purposes.

5. Limiting use, disclosure and retention

- Organizations may use and disclose personal information only for identified purposes.
- Organizations may keep personal information only as long as they need it for identified purposes. They must then destroy it.
- If an organization uses personal information to make a decision about an individual, they must keep the information long enough for the individual to have access to the information after the decision has been made.

6. Accuracy

- The use of the information determines how accurate and up-to-date the information must be.

- Organizations may not update information routinely unless necessary.

7. Safeguards

- Organizations must keep personal information secure and restrict access to it.

8. Openness

- Organizations must provide information about their policies on the management of personal information. They must indicate who in the organization is responsible to ensure compliance with PIPA (for example, personal information protection policy posted on website).

9. Individual access

- When asked, organizations must tell individuals what personal information is held about them and they must allow the individual to check the accuracy of the information.
- The organization must correct inaccurate information.

10. Challenging compliance

- Organizations must have a procedure in place to receive and handle complaints about how they collect and use personal information.