ABTA
Data Management Principles

The Asia Business Trade Association recognizes that companies should have in place appropriate data management principles to protect customer, company, employee and third party data. Such principles should apply to firms of all sizes, although the way in which they are adhered to will differ depending on the size of the company and the sensitivity of the data collected.

1. Establish company data management policies that distinguish between different types of data through a data classification system.

2. Attribute different levels of protection and handling to data according to its sensitivity.

3. Classify information into two distinct groups – public and internal – with extra protections given to more sensitive data. For example:
   - Public information that is freely available outside the firm and intended for public distribution should not have any associated information handling requirements.
   - Internal information that is shared within the company and not intended for distribution outside – such as management policies or employee email addresses – should have specific handling requirements, such as disposal only at a secure company location.
   - More sensitive internal information that could have a significant negative impact on a customer if disclosed – such as biometric data or information on race, religion or political affiliation – should have a much stricter set of information handling requirements for collection, transmission, storage and disposal, such as encryption at all times.

4. Companies should also distinguish between Personally Identifiable Information (PII) and non-Personally Identifiable Information (non-PII) to protect the privacy of individuals.

5. Have a process in place to monitor and approve cross-border data transfers and ensure privacy and security are upheld.

6. Assign a person within the firm to be responsible for data management reporting to senior management.

7. Data should be allowed to flow across borders if companies can demonstrate sufficient data management policies are in place to ensure privacy, security and access to data, even if it is offshore.

8. Restrictions on the free-flow of data should not apply to sectors and only be considered if a firm has not adhered to regulatory or legal requirements.

9. Given the interconnectedness of countries across Asia – and around the world – the need for a high degree of consistency in data classification regimes across jurisdictions is also important to allow for data transfers.