Module	**Japan – Privacy and Data Protection**
Jurisdictions	**Japan**

Module Application

Does the organisation engage in business operations that involve the collection, storage, processing, or transfer of personal data, particularly in the context of offering goods or services to individuals within Japan?

Does the organisation have mechanisms in place to ensure compliance with data privacy obligations under the Act on the Protection of Personal Information (APPI), including data minimisation, security measures, and data breach notification protocols?

Does the organisation manage specific categories of sensitive personal data, such as information related to social security, taxation, or healthcare, thereby requiring adherence to stricter privacy safeguards under the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures?

Module Scope

The module provides organisations with a comprehensive framework for complying with legal obligations related to personal data protection as outlined in the APPI. This module also encompasses specific guidelines and regulations concerning sensitive data categories, including Specific Personal Information, managed under the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures.

This module offers practical guidance to establish and maintain best practices for data protection and privacy compliance. While organisations are not explicitly mandated to implement comprehensive data protection systems, the adoption of such measures is strongly recommended as a best practice approach.

Key requirements:

1. Collection, processing, and use of personal information:
    - Personal data must be collected and processed only for the disclosed purposes agreed upon by the data subject. Any change in purpose requires renewed consent from the data subject.
    - Adequate measures must be implemented to prevent data leaks, unauthorised access, and misuse of personal data.
2. Handling of specific personal information:

- Organisations managing Specific Personal Information (e.g., data related to social security or taxation) must comply with stricter rules and safeguards outlined in the relevant legislation.
- Stringent guidelines govern the acquisition, storage, access, and transfer of such sensitive data.

3. Data transfer restrictions:
   - Transfers of personal data to third parties, including cross-border transfers, are subject to stringent controls. Explicit consent from data subjects is required unless specific exemptions apply.
   - The organisation must ensure that third-party recipients adhere to equivalent data protection standards.
4. Data security and breach management:
   - Robust data security measures must be established to safeguard personal data from potential breaches.
   - In case of a data breach, organisations are required to promptly notify affected data subjects and take measures to mitigate damage and prevent future occurrences.
5. Record-keeping and accountability:
   - Accurate records of personal data processing activities must be maintained to demonstrate compliance with legal obligations.
   - Organisations must maintain transparency with data subjects and regulatory bodies, ensuring that data processing practices align with legal standards.

Practical guidance

Organisations are encouraged to implement internal policies and procedures that align with the APPI and other relevant laws and guidelines, including:

- Data Minimisation and Consent: Personal data should be limited to what is necessary for the intended purpose, and data subjects must provide informed consent for data collection and processing.
- Data Security Controls: Implement security measures, including encryption, access controls, and data anonymisation where appropriate, to safeguard personal information.
- Third-Party Management: Ensure that third-party service providers adhere to the organisation's privacy policies and legal obligations for data protection.
- Data Subject Rights: Facilitate data subject rights, including access, correction, deletion, and data portability, as mandated under applicable laws.

Compliance sources

- Act on the Protection of Personal Information (APPI)
- Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures
- General Rules Guidelines for the Act on the Protection of Personal Information
- Guidelines on Anonymously Processed Information and Third-Party Data Provision

Consequences of non-compliance

Non-compliance with data protection obligations can lead to:

- On-site inspections by the Personal Information Protection Commission (PPC) may be conducted, and organisations may be required to submit compliance reports.
- Guidance, recommendations, and orders from the PPC. Non-compliance with such orders may lead to imprisonment of up to six months or fines up to ¥300,000.
- Legal liability may extend to both responsible individuals and the corporate entity.
- Organisations may face civil claims for damages due to non-compliance with data protection obligations.

About LexisNexis Regulatory Compliance®

LexisNexis Regulatory Compliance® helps you forge a clear path to compliance.

With LexisNexis® content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.
