

Background to the Guidebook for Corporate Privacy Governance in the Digital Transformation (DX) Era Ver 1.3

<International trends (Actions by the EU and the U.S.): Growing impact of privacy on corporate value>

- **Many business leaders** in the EU and the United States **recognize that they should deal with privacy issues as a management issue**, against the backdrop of government enforcement of a large amount of fines and penalties for violators from the perspective of the fundamental human rights of individuals under the General Data Protection Regulation (GDPR) in the case of the EU and that of the protection of consumers under Article 5 of the Federal Trade Commission Act in the case of the U.S.
- **GDPR** stipulates provisions requiring business enterprises to establish an internal system, e.g., **appointment of an independent Data Protection Officer (DPO)**.
- In this circumstance, **some companies** have begun to ascertain privacy as part of their management strategies and appropriately address privacy issues, thereby **gaining social trust and leading to improvement of corporate value**.

<Domestic trends:

Actions by Japanese business enterprises playing a leading role worldwide and their responses to the amendment of the Act on the Protection of Personal Information (APPI) >

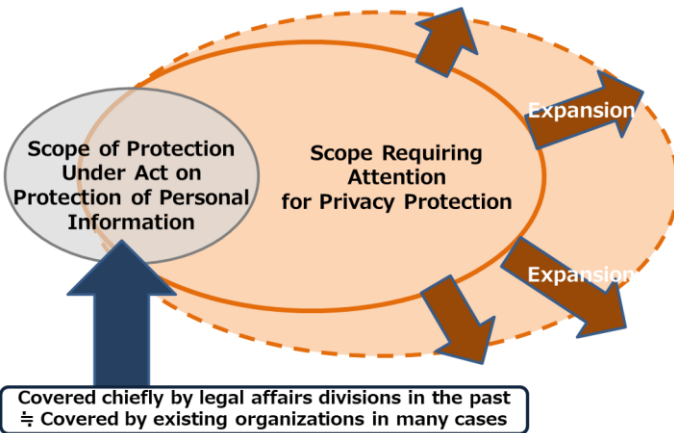
- Also from the viewpoint of Japan's realization of the Data Free Flow with Trust (DFFT) policy for economic growth brought about by international data flows, data security and privacy should be ensured in order to gain trust from the public and enhance trust between business enterprises. Against this backdrop, Japanese business enterprises, as well, need to **pay attention to the level of data security and privacy that overseas business enterprises are required to meet**.
- **The Outline of Revision of the Systems related to APPI** states that Japan should further promote **efforts led by the private sector**, in particular, in the fields utilizing digital technologies. As part of these efforts, the outline **recommends business enterprises to take voluntary efforts, e.g., appointing person in charge of the handling of personal data and implementing a privacy impact assessment (PIA)**.

Background to the Guidebook for Corporate Privacy Governance in the Digital Transformation (DX) Era Ver 1.3

- As business models have been dramatically changing and technical innovations have been rapidly progressing in recent years, business enterprises engaging in data transformation (DX), which are playing a central role in innovations, **should take action to reduce the variety of risks that emerge from this innovation.**
- Business enterprise’s concern in conducting business with attention to privacy issues has been centered on compliance with the APPI until now.—Nevertheless, some business enterprises, even if they comply with laws and regulations, cause social media “flaming” resulting from their being unable to avert **criticisms of their responses to privacy issues** with such responses considered insufficient to address discrimination against, disadvantages for and anxiety of consumers. Such criticism, in some cases, **results in a serious problem threatening the continuance of the business enterprises.**
- Companies should **actively make responses to privacy issues**, proactively fulfill accountability for consumers and stakeholders and **gain trust from society.** The business leaders should consider approaches to facing privacy issues as an important part of corporate strategies, which may lead to improving corporate value.

Scope of attention required from the viewpoint of privacy protection and establishment of a system therefor

The scope of attention required from the standpoint of privacy protection is not limited to the scope of protection under Act on Protection of Personal Information in view of the importance of the protection of consumers and of privacy. Special caution must be exercised due to changes that take place in the information to be handled, in technologies and in the environment.



Along with innovation, the scope of matters to be considered from the viewpoint of privacy protection(privacy issues) is expanding.

It is needed that a system be established that can consider the entire privacy issue.

Communication with stakeholders



Toward business enterprises’ establishment of privacy governance for gaining social trust,
MIC and METI organized the basics which business enterprises should begin with in the guidebook.

Overview of the Guidebook for Corporate Privacy Governance in the Digital Transformation (DX) Era Ver 1.3

Target readers: The following personnel working for: a business enterprise who are likely to receive requests for attention to privacy directly from consumers while offering their products and services, etc., by utilizing personal data, and for vendors that conduct trade with these business enterprises; or other business:

[i] **Business leaders and managers in the position of submitting proposals to such business leaders, etc.**

[ii] Employees in business divisions responsible for comprehensive management of matters concerning data utilization, its application, and protection, etc.

The Three Requirements to Be Addressed by Business Leaders

Requirement 1: Explicit Statement of the Corporate Stance on Privacy Governance

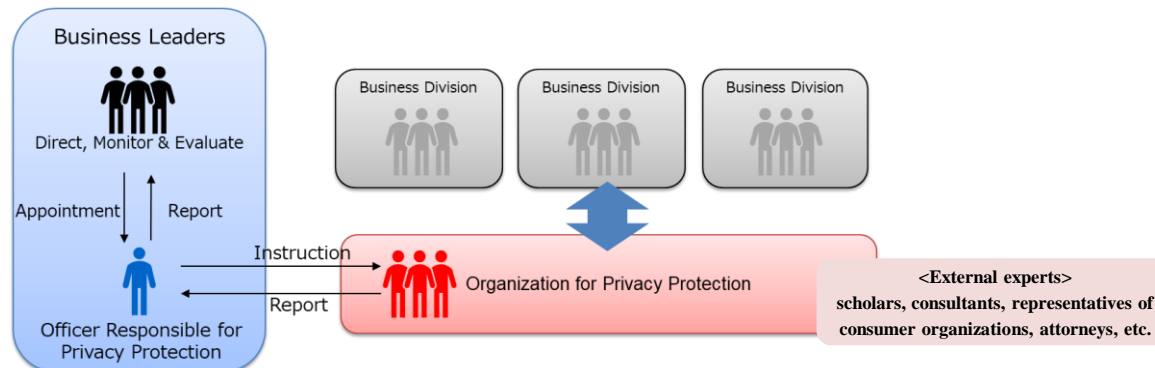
Business leaders need to recognize protection of consumer privacy as one of the important management issues and state explicitly their basic policy and their stance focused on privacy protection. Business leaders also need to communicate awareness of the corporate policy and their stance both inside and outside of their organization. Business leaders are required to ensure accountability for implementing privacy-related activities based on the announcement that has been explicitly made.

Requirement 2: Appointment of the Officer Responsible for Privacy Protection

Business leaders need to appoint a person to take charge of privacy-related activities across their organization (hereinafter "Officer Responsible for Privacy Protection"), identify the scope of the officer, and grant the officer authority for executing the countermeasures to appropriately prevent privacy issues from arising.

Requirement 3: Investment of Resources in Privacy-Related Activities

Business leaders are required to invest the necessary and adequate quantity of management resources (people, goods, money, etc.). It is necessary to establish a system for privacy and to allocate adequate manpower and assure human resource development, including manpower recruitment.



References:
Approaches to Responding Privacy Risks (e.g., PIA), Information Collecting Methods in Relation to Foreign Laws and Regulations, etc., Privacy by Design

Key Items in Privacy Governance

- 1. Establishing a system for privacy**
(internal control, establishing an organization for privacy protection, and collaboration with external experts)
- 2. Establishment and Dissemination of Management Rules**
(establishing rules for exhaustive implementation, disseminating and entrenching the rules throughout the business enterprise)
- 3. Cultivation of Corporate Culture Pertaining to Privacy**
(cultivating a corporate culture for each employee to be aware of privacy-related issues as one's own)
- 4. Communication with consumers**
(announcing publicly privacy-related activities of the business enterprise, communicating with consumers continuously)
- 5. Communication with other stakeholders**
(communication with business partners, group companies, etc., investors and shareholders, administrative organizations, industry organizations, employees and others)

Improving corporate value and business advantages

Gaining social trust

Consumers and other stakeholders

Reference:
Examples of efforts for privacy governance

