

# Cyber Incident Response and Data Breach Notification (Japan)

by [Hiroyuki Tanaka](#), [Noboru Kitayama](#), and [Naoto Shimamura](#), Mori Hamada & Matsumoto, with Practical Law Data Privacy & Cybersecurity

---

Practice notes | [Law stated as of 01-Nov-2024](#) | Japan

---

A Practice Note addressing key legal requirements and considerations when handling data breaches, cyberattacks, or other information security incidents in Japan or drafting data breach response notifications regarding personal data originating from Japan. This Note also discusses guidance from the Personal Information Protection Commission (PPC) and obligations under the Act on the Protection of Personal Information (APPI), the Basic Act on Cybersecurity, and sector-specific laws and regulations. The Japan-specific guidance in this Note may be used with the generally applicable resources listed in the [Global Cyber Incident Response and Data Breach Notification Toolkit](#).

---

Data breaches, cyberattacks, and other information security incidents are increasingly common across sectors and affect a wide range of large and small organizations. In response, data breach notification laws, regulations, and best practices raise significant challenges for global companies. This Note explains the Japanese laws and regulations an organization must consider and the local resources available when handling data breaches of personal data originating from Japan.

Cyber incidents occur when events compromise the security, confidentiality, integrity, or availability of an information technology (IT) system, network, or data. Reporting and notification obligations vary according to a cyber incident's characteristics. For example:

- Data breach notification obligations may apply if the event exposes personal information to potential unauthorized access or use.
- Other cyber incident notification requirements may apply if the event affects critical infrastructure or regulated entities.

Some cyber incidents result from criminal activities. Victimized organizations should consider reporting cybercrime to applicable authorities.

The Japan-specific guidance in this Note may be used with the generally applicable resources listed in the [Global Cyber Incident Response and Data Breach Notification Toolkit](#).

## Data Breach Notification

Several Japanese laws and related guidance address notification for data breaches of personal information, including:

- The [Act on the Protection of Personal Information](#) (APPI), which generally regulates personal data collection, use, and disclosure. The APPI did not previously require data breach notification. However, amendments to the APPI that took effect on April 1, 2022 require mandatory data breach notification to the [Personal Information Protection Commission](#) (PPC) under certain circumstances.

(See Data Breach Notification Requirements Under the APPI.)