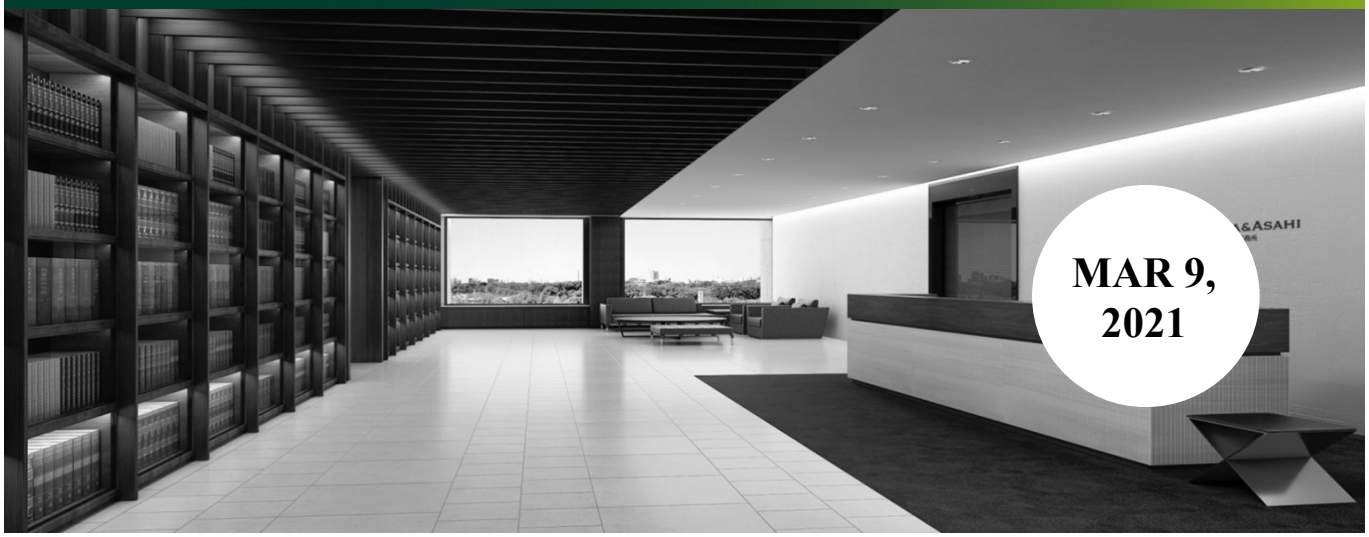
西村あさひ法律事務所

NISHIMURA & ASAHI

Data Protection Newsletter



Proposed Amendment to the Ministerial Ordinances of the Act on the Protection of Personal Information of Japan: Data Breach Notification (Part II)

Noriya Ishikawa, Akiko Takiguchi

In Part II of this series, we will address the details of the data breach notification in the case of Data Breach Incidents. Please refer to Part I to this newsletter for a general introduction of the proposed amendment to the ministerial ordinances of the Act on the Protection of Personal Information ("**APPI**").[1] *The amendment to the ministerial ordinances of the APPI was finalized and published on March 24, 2021. There are no changes from the proposal.

Under the 2020 Amendment, the current framework (non-legally binding reporting and notification obligation) is replaced with legally binding and enforceable obligations. The 2020 Amendment provides that when any leak or loss of, or damage to, personal data processed by a business operator or any other incident concerning the security of personal data (each, a "**Data Breach Incident**") occurs and such Data Breach Incident is highly likely to cause harm to the rights and interests of a data subject, the business operator shall (i) report the Data Breach Incident to the Personal Information Protection Committee ("**PPC**") and (ii) notify the relevant data subjects of the Data Breach Incident in accordance with the Enforcement Rules for the APPI. The purpose of the report to the PPC is so that the PPC is aware of the situation as soon as possible and can take necessary measures for the Data Breach Incident, and the purpose of the notification to the relevant data subjects is so that the data subjects acknowledge the Data Breach Incident and can take measures to protect their rights and interests.

(1) Report and Notification Criteria

The proposal of the Enforcement Rules provides what kinds of events would fall under Data Breach Incidents that are highly likely to cause harm to the rights and interests of a data subject and require a business operator to report to the PPC and notify the relevant data subjects. Taking into account the nature of the personal data, the likely consequences of the Data Breach

[1] https://www.nishimura.com/en/newsletters/data_protection_210303.html

Incident, the manner in which the Data Breach Incident occurs, and the scale of the Data Breach Incident, the duty to report to the PPC and notify the relevant data subjects would apply in case of a Data Breach Incident that:

- relates to personal data containing special care-required personal information (personal information comprising a data subject's race, creed, social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the data subject);
- is likely to cause proprietary damage by unauthorized use of personal data;
- may have occurred for the improper purpose; or
- involves personal data of more than 1,000 data subjects.

These categories should be the exhaustive list. The business operator does not have to assess whether the rights and interests of a data subject are compromised, unlike the rules under the GDPR. For example, cyber-attack cases should in most cases fall within the third category. However, if personal data affected by a Data Breach Incident is secured by advance encryption and other measures necessary to protect the rights and interests of the data subject of the personal data, the duty to report to the PPC and notify the relevant data subjects would not apply. Encryption is becoming important in Japanese data privacy practice as well.

Unlike the rules under the GDPR, the criteria for reporting to the PPC and notifying the relevant data subjects are the same. Please note that all of the above Data Breach Incidents include not only Data Breach Incidents that have already occurred but also Data Breach Incidents that may have occurred.

(2) Timing and format of the reports and notifications

The proposal also sets forth some requirements for the reports and notifications. Unlike the rules under the GDPR, the proposal does not provide the specific time limit within which a business operator must submit a report and provide notice concerning a Data Breach Incident. Instead, the proposal establishes a two-stage deadline applicable to initial reports and final reports. Under the proposal, the initial report must be made by a business operator to the PPC promptly after becoming aware of the Data Brach Incident and must contain the following information (limited to those of which a business operator is aware at the time of the report):

- an outline of the Data Breach Incident;
- the affected personal data;
- the number of affected data subjects;
- the cause of the Data Breach Incident;
- whether any secondary damage is likely to occur, and if any, the details of the secondary damage;
- the status of implementation of communications with the affected data subjects and a public announcement;
- the measures for preventing recurrence; and
- other matters for reference.

The guidelines, which are currently being revised by the PPC, will likely provide some guidance on the timing of making initial reports for reference purposes.

The proposal further provides that final reports must be made within 30 days (or, in the case of a Data Breach Incident which may have occurred for the improper purpose, 60 days) after the date when a business operator becomes aware of the Data Brach Incident and must contain the items described above. Together, under the proposal, a business operator shall notify the relevant data subjects of certain items described above (i.e., an outline of the Data Breach Incident, the affected personal data, the cause of the Data Breach Incident, whether any secondary damage is likely to occur, and if any, the details of the secondary damage,

and other matters for reference) to the extent necessary to protect the data subjects' rights and interests promptly (depending on the situation of the Data Breach Incident) after becoming aware of the Data Brach Incident. The difference between the requirements for reports and notifications stem from the different purposes thereof.

(3) Rules for the entrusted party (data processor)

Although the APPI does not have the concept of data controller and data processor, if a business operator who is entrusted by another business operator to process personal data notifies a Data Breach Incident to the entrusting business operator, they are exempted from the duty to report to the PPC and notify the relevant data subjects. The proposal provides that in order to be exempted from the duty, the business operator shall notify the entrusting business operator of the items described above promptly after becoming aware of the Data Brach Incident.

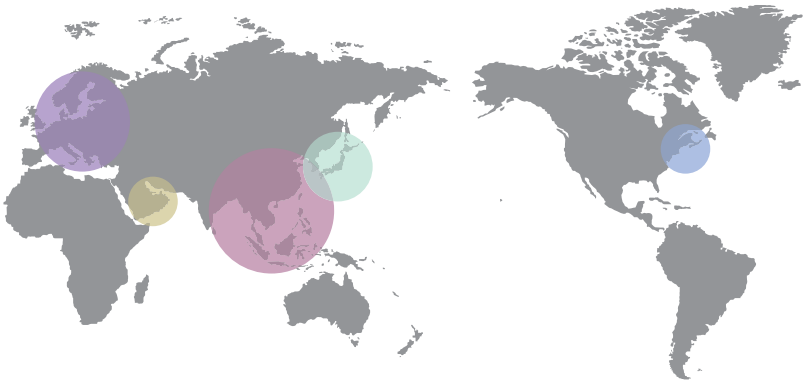
Noriya Ishikawa
Partner, Frankfurt & Düsseldorf Offices Co-Representative
E-mail: n.ishikawa@nishimura.com

Noriya Ishikawa serves as co-representative of our offices in Frankfurt and Düsseldorf, Germany. He advises national and international clients from various industries, in particular with regard to projects involving multi-national data protection law issues, such as drafting policies, data transfer agreements, and outsourcing agreements, as well as IT compliance questions and data breach issues. He was awarded first place in the Nikkei's "**Most Successful Lawyers in 2019**" in the Area of Data Protection. The Nikkei, Japan's flagship economics newspaper and owner of the Financial Times, publishes this highly-regarded annual survey ranking Japan's most outstanding lawyers across specific categories.

Akiko Takiguchi
Attorney-at-Law
E-mail: a.takiguchi@nishimura.com

Akiko Takiguchi is an associate at Nishimura & Asahi. She is admitted to practice in Japan (2010) and mastered LL.M. of New York University in 2018. She has represented Japanese and international clients in various corporate law matters, including cross-border and domestic M&A transactions and general corporate issues.

Nishimura & Asahi has 18 offices throughout Japan and in the markets that matter, with Asia as the starting point.



Tokyo

Otemon Tower, 1-1-2 Otemachi, Chiyoda-ku, Tokyo 100-8124 Japan

Tel +81-3-6250-6200 +81-3-6250-7210 (Nishimura & Asahi LPC Principal Office)

Nagoya

Tel +81-52-533-2590

LPC Partner Hiroki Fujii

Osaka

Tel +81-6-6366-3013

LPC Partners Hiromune Usuki
Taisuke Igaki
Yuichiro Hirota
Masanori Ban

Fukuoka

Tel +81-92-717-7300

LPC Partners Tsuneyasu Ozaki
Kengo Takaki
Yasuko Maita

New York

Nishimura & Asahi NY LLP

Tel +1-212-830-1600
E-mail info_ny@nishimura.com
Managing Partner Katsuyuki Yamaguchi
Vice Managing Partner Megumi Shimizu
Partners Kaoru Tatsumi
Yusuke Urano

Dubai

Tel +971-4-386-3456
E-mail info_dubai@nishimura.com
Counsel Masao Morishita

Frankfurt (main office)

Nishimura & Asahi Europe
Rechtsanwaltsgesellschaft mbH

Tel +49-(0)69-870-077-620

Düsseldorf (branch office)

Nishimura & Asahi Europe
Rechtsanwaltsgesellschaft mbH

Tel +49-(0)211-5403-9512

E-mail info_europe@eml.nishimura.com
Co-representatives Noriya Ishikawa
Dominik Kruse

Bangkok

Tel +66-2-168-8228
E-mail info_bangkok@nishimura.com
Partners Hideshi Obara
Chavalit Uttasart
(SCL Nishimura)
Jirapong Sriwat
Tomoko Shimomukai

Jakarta*1

Walalangi & Partners

Tel +62-21-5080-8600
E-mail info@wplaws.com
Representative Luky Walalangi

Rosetini & Partners Law Firm

Tel +62-21-2933-3617
E-mail info_jakarta@nishimura.com
Partner Noriaki Machida

Yangon

Tel +95-1-8382632
E-mail info_yangon@nishimura.com
Representative Yusuke Yukawa
Vice Representative Isamu Imaizumi

Beijing

Tel +86-10-8588-8600
E-mail info_beijing@nishimura.com
Chief Representative Azusa Nakashima
Representative Masashi Shiga

Shanghai

Tel +86-21-6171-3748
E-mail info_shanghai@nishimura.com
Chief Representative Takashi Nomura
Representatives Satoshi Tojo
Seita Kinoshita

Singapore

Tel +65-6922-7670
E-mail info_singapore@nishimura.com
Co-representatives Masato Yamanaka
Shintaro Uno
Partners Masataka Sato
Yuji Senda
Ikang Dharyanto

Note: We are in formal law alliance with Bayfront Law LLC, a Singapore law practice, under name of Nishimura & Asahi-Bayfront Law Alliance.

Okada Law Firm (Hong Kong)*2

Tel +852-2336-8586
E-mail s.okada@nishimura.com
Representative Saori Okada

Hanoi

Tel +84-24-3946-0870
E-mail info_hanoi@nishimura.com
Partner for Vietnam offices Hikaru Oguchi
Representative Akira Hiramatsu

Ho Chi Minh City

Tel +84-28-3821-4432
E-mail info_hcmc@nishimura.com
Partner for Vietnam offices Hikaru Oguchi
Representative Kazuhide Ohya
Partners Vu Le Bang
Ha Hoang Loc

Taipei

Nishimura & Asahi Taiwan

Tel +886-2-8729-7900
E-mail info_taipei@nishimura.com
Co-Representatives Ing-Chian Sun
Sheng-Chieh Chang

*1 Associate office *2 Affiliate office