NISHIMURA & ASAHI

DIJ Web-Forum

Data and Values

June 10, 2021

Hitomi Iwase

Introduction

NISHIMURA & ASAHI

Hitomi Iwase

Partner
Attorney-at-Law, admitted in Japan and New York
TEL: +81-3-6250-6218 (Direct)
Email: h.iwase@nishimura.com

Practice Areas:

- IP/IT/Data Privacy

Education:
Waseda University (LL.B.)
Stanford Law School (LL.M.)

Ms. Hitomi Iwase is a partner at Nishimura & Asahi specializing in the areas of intellectual property (IP), information technology (IT) and data privacy. She handles patents, copyrights, trademarks, trade secrets and other IP-related matters in multiple business sectors, including IT, life sciences and healthcare, machinery, food, fashion, environment and energy, entertainment, financial services, and e-commerce. Ms. Iwase's expertise encompasses all forms of IP transactional work, both cross-border and domestic, including licensing, strategic alliances, joint development, and asset transfers, as well as various types of IP disputes, including patent/trademark infringement litigation. She also assists clients in anti-counterfeiting and in the development of IP portfolios and prosecution strategies. Ms. Iwase regularly advises clients on emerging legal issues relating to the latest technology, such as IoT and artificial intelligence (AI), as well as on complex system-related transactions and disputes over those transactions. In the area of data privacy, Ms. Iwase extensively provides advice on data protection and privacy compliance, including on establishment of global compliance systems as well as incidents such as data breaches. Ms. Iwase also advises on related areas such as e-commerce, advertising, and consumer protection.

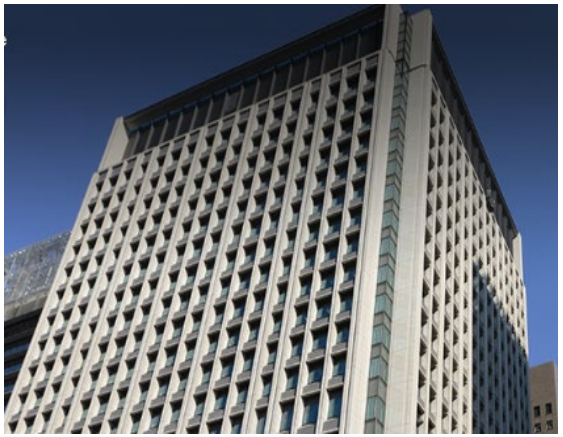
Introduction – Nishimura & Asahi

NISHIMURA & ASAHI

- Largest law firm in Japan, with more than 700 attorneys, including patent & trademark attorneys and foreign attorneys / approximately 1,700 personnel in total.

- 4 offices in Japan, and 14 offices (including 2 offices in Germany), including representative offices, outside Japan.

*For details: https://www.nishimura.com/en



Privacy Law in Japan - APPI

NISHIMURA & ASAHI

Act on the Protection of Personal Information (個人情報保護法)

- Key piece of legislation governing personal information in Japan
- Purpose: to balance the rights and interests of individuals v. use of personal information
- Enacted in 2004 and became fully effective in 2005; the first amendment came into full effect on May 30, 2017, and the latest amendments were in 2020 and 2021
- Provides general rules concerning the protection of personal information in the private sector (regulates the handling (collection, storage and use) of personal information), as well as protocols for the government
  - Details are clarified through common guidelines promulgated by the Personal Information Protection Commission (PPC)
  - Enforced by the PPC
  - The PPC can request a report, conduct investigations, and may issue instructions or orders

Japanese Privacy Laws

NISHIMURA & ASAHI

Constitution / Court Precedent

Act on the Protection of Personal Information (個人情報保護法)

Basic data protection policies (Ch. 1-3)

Rules applicable to the private sector (Ch. 4-7)

[Details are clarified through common guidelines promulgated by the Personal Information Protection Commission (PPC)]

Act on the Protection of Personal Information Held by Administrative Organs (行政機関個人情報保護法)

Act on the Protection of Personal Information Held by Independent Administrative Agencies (独立行政機関個人情報保護法)

Ordinances on the protection of personal information established by local governments

Businesses handling personal information in the private sector

National government

e.g. National Hospital Org., National University Hospital

Local governments, including municipal hospitals

Data Protected under the APPI

NISHIMURA & ASAHI

- Three categories → different rules apply
  - **Personal information (PI) (個人情報)**
    - Information about a living individual that falls under any of the following items:
      i. information containing **a name, date of birth or other descriptions whereby a specific individual can be identified** (including **information that allows easy reference to other information that would thereby enable identification of the individual**); or
      ii. information containing **an individual identification code**, which is a code, including characters, numerical characters and marks, that can be used to identify a specific individual and which is specified in a cabinet order (e.g., biometric identifiers such as fingerprint data or facial recognition data, passport or driving licence numbers).

    * IP addresses and cookie IDs typically do not fall under Personal Information.
  - **Personal data (PD) (個人データ)**
    - personal information contained within a personal information database
    - "personal information database" = a collection of information
  - **Retained personal data (RPD) (保有個人データ)**
    - personal data that a business operator has the authority to disclose, correct, discontinue the use of, erase, etc.

Overview of Obligations under the APPI

NISHIMURA & ASAHI

Obligations of Business Handling PI		PI	PD	RPD
Purposes of use	Specify purposes of use			
	Purpose restrictions			
	*No improper use			
Collection	Proper collection			
	Notify or publicly announce the purposes of use			
Management	Keep accurate and up to date, etc.			
	Security control measures			
	Supervision over employees			
	Supervision over service providers			
	*Breach notification			
Provision to others	Restriction on provision to third parties			
	Restriction on provision to third parties located outside Japan			
	Confirmation and record obligations			
Data subject rights	Disclosure			
	Correction, deletion, etc.			
	Cease use/provision to third parties			

Rules regarding Cross-Border Data Transfer

NISHIMURA & ASAHI

- **General rule:** You cannot provide personal data to third parties located in a foreign country without the subject individual's prior consent
  - when transferring personal data to a third party (including group companies) in a foreign country, in general, consent from the data subject is required

- **Exceptions:** Provision to a third party with a management system conforming to the standards set out in the PPC rules:
  - recognition by the APEC Cross-Border Privacy Rules (CBP)
  - when the parties ensure compliance with relevant provisions of the APPI by taking appropriate and reasonable measures -- by a data transfer agreement (similar to the concept of SCC under EU law) or intercompany rules (similar to the concept of BCR under EU law)
  - to a country that is designated by the PPC as having legislation equivalent to the APPI (currently the EEA and the UK) ← **Japan's adequacy decision**

Harmonization and Data Free Flow

NISHIMURA & ASAHI

- "Data Free Flow with Trust" (DFFT) -- Former Prime Minister Abe's speech at the Davos World Economic Forum in January 2019
  - Digital data will increasingly be the engine for growth
  - We must, on one hand, be able to put our personal data and data embodying intellectual property, national security intelligence … under careful protection, while on the other hand, we must enable the free flow of medical, industrial, traffic and other most useful, non-personal, anonymous data to see no borders.
- More harmonization?

NISHIMURA&ASAHI