



Alpine Privacy Days

**Developments in Japanese privacy law &
AI and Metaverse Concerns**

Takashi NAKAZAKI

March 8, 2024

Today's Topics

- I. Developments in Japanese privacy law
- II. Privacy risks of AI
- III. Privacy concerns on the Metaverse

I-1. PPC's interview with EBC

<PPC plans to amend the APPI>

- Japan's data protection authority, Personal Information Protection Commission (PPC), reviews the Act on the Protection of Personal Information (APPI) every three years and had conducted opinion hearings from many relevant domestic and foreign organizations.
- European Business Council (ECB) represents European business sector interests in Japan.
- PPC interviewed the ECB in autumn 2023 to find out what complaints they had about the APPI.

I-1. PPC's interview with EBC

<Definitions>

- GDPR and APPI both deal with personal information but use different definitions which often lead to insecurity of European and Japanese businesses using personal information in Europe and Japan even if the application of the definitions leads to the same result.
- “Personal Data” (GDPR) vs. “Personal Information” (APPI)
- “Processing” (GDPR) vs “Handling” (APPI)
- EBC suggested harmonization of definitions between the GDPR and the APPI to the extent feasible.

I-1. PPC's interview with EBC

<Legal Basis of Processing Personal Information>

- GDPR requires a legal basis for processing of personal information (Article 6 GDPR) which includes various options, such as consent (Article 6(a)), the necessity for the performance of the contract (Article 6(b)), processing is necessary for compliance with a legal obligation (Article 6(c)), processing is necessary for the purposes of the legitimate interest (Article 6(f)), etc.
- In Europe, the majority of businesses uses the so-called “legitimate interest” as legal basis for processing personal information, including the transfer of personal information to third parties.

I-1. PPC's interview with EBC

<Legal Basis of Processing Personal Information>

- While in Japan the handling of personal information is legally feasible as long as the handling takes place within the purpose of use notified to the data subject, the transfer of personal information to a third party in principle requires a consent.
- In Europe, a consent is considered one of the weakest legal basis for processing of personal information because (i) the consent may be legally invalid as the requirements to obtain legal consent are very strict and (ii) it can be withdrawn by the data subject at any time for the future.

I-1. PPC's interview with EBC

<Legal Basis of Processing Personal Information>

- Therefore, European businesses wish to use a different legal basis for a transfer of personal information.

I-1. PPC's interview with EBC

<Legal Basis of Processing Personal Information>

- Disadvantages due to different legal basis in GDPR and APPI:
- European Businesses need to amend privacy policies for Japan to delete “legitimate interest” as legal basis for data processing which leads to higher administrative costs and possibly less reliable legal basis of consent;
- Obtaining consent further increases administrative costs of businesses;
- Even after a merger often a consent needs to be obtained if personal information shall be used beyond the scope of the original purpose of use;

I-1. PPC's interview with EBC

<Legal Basis of Processing Personal Information>

- A simple transfer of personal information between group entities is difficult without consent, unless the personal information is “jointly used” from the time of collection, a concept which is unknown in the GDPR;
- Japanese businesses in Europe often rely on “consent” as legal basis for data processing even though it is considered the weakest legal basis in Europe, often resulting in the consent of the data subject being legally invalid.
- EBC suggested introduction of a concept of “legitime interest” in the APPI.

I-1. PPC's interview with EBC

<Extraterritorial Application of APPI>

- The APPI applies extraterritorially to businesses in Europe collecting personal information from data subjects in Japan in connection with the provision of goods or services to individuals in Japan, while many regulations can still be considered stricter under the GDPR, e.g. the data processing already requires a legal basis and not only the notification of the purpose of use and the obligation of a controller to notify data breaches within 72 hours etc.
- This means that European businesses as described above need to apply both, the GDPR and APPI standard.

I-1. PPC's interview with EBC

<Extraterritorial Application of APPI>

- Suggestion: In case of the European Economic Area (EU member states, Norway, Liechtenstein and Iceland) apply only GDPR to such businesses which handle personal information of individuals located in Japan in connection with the provision of goods or services once the legal basis of processing of personal information has been unified between the GDPR and the APPI.

I-2. Other Major Differences between GDPR and APPI

<Other major differences>

- “controller” vs “processor”
- “right to erasure”
- Sanction

I-3. Interim report on the amendments of APPI

<PPC's review of APPI>

- PPC reviews APPI every 3years.
- PPC issues the interim report on the amendments of APPI on 15 November. 2023.
- Several topics are disclosed in the interim report.

I-3. Interim report on the amendments of APPI

<PPC's Interim Report>

- Three perspectives on the revision study
- (i) More substantial protection of individual rights and interests.
- (ii) Effective monitoring and supervision.
- (iii) The state of support for efforts to make use of data.

I-3. Interim report on the amendments of APPI

<Main opinions on the status of PPC's enforcement.>

- The acquisition of personal data should only be limited to the minimum necessary in relation to its intended purpose.
- The approach should be examined in light of social changes accompanying technological developments, such as the spread of generative AI and authentication technologies, so that the discipline on the 'prohibition of improper use' can take a more effective form.
- In addition, conditionality and other factors should be considered when granting cloud exceptions in light of the actual safety management measures taken in recent leakage and other cases.

I-3. Interim report on the amendments of APPI

<Main opinions of the Status of PPC's enforcement.>

- Consideration should be given to the use of individual data, including screening during its creation and the range of subjects who can access the data.
- The state of protection of children's rights and interests should be examined, taking into account trends in discussions in other countries.
- While working on designing a system that is easy for the general public and companies to understand and fostering literacy, specific goals should be discussed on how leaks should be reported and what kind of enforcement should be carried out by the Commission.

I-3. Interim report on the amendments of APPI

<Main opinions on the status of PPC's enforcement.>

- Consideration should be given to whether the gap between private and public discipline hinders the sharing of necessary personal information.
- Class actions should be considered from the perspective of increasing avenues for the protection of individual rights and interests, although practical problems exist.

I-3. Interim report on the amendments of APPI

<Main opinions on the status of PPC's enforcement.>

- In order to make rights remedies more effective, consideration should be given to strengthening direct penalties, introducing a surcharge system and using emergency orders.
- The concept of consent should be elaborated in order to protect substantive rights and interests.
- While consideration should be given to ensuring that the strengthening of penalties does not hinder companies' use of personal data, even if penalties are increased, the extent of the increase and other factors should be carefully considered.

I-3. Interim report on the amendments of APPI

<Main opinions on the status of PPC's enforcement.>

- Cooperation with the relevant ministries should be further enhanced with regard to analysis of leakage incidents.
- The daily occurrence of leaks, etc. identified through mandatory reporting of leaks, etc., should be analysed and effective measures to prevent them should be considered.
- The possibility of deterring misuse and protecting rights and interests through the protection of personal data should also be considered for events that the Personal Data Protection Act alone has limited capacity to address, such as misuse of personal data for criminal purposes and generated AI.

II-1. Privacy risks of AI

<Guidelines related to AI>

- AI governance guidelines (2022)
- New “AI Guidelines for Business” (March, 2024)

II-1. Privacy risks of AI

<Legal risk>

- Learning and prompt input of personal information (purpose of use, provision to third parties, cross-border transfers) (Reference: Cloud Exception)
- Collecting sensitive personal information for training data
- Utilization purposes

II-1. Privacy risks of AI

<Privacy risk>

- “AI Guidelines for Business” will be published by METI and MIC in mid of March, 2024
- New AI guidelines focus on privacy issues as following:
 - Automated decision making
 - Working place monitoring by AI camera
 - Bias

II-2. PPC's alerts against OpenAI

<PPC's Alert on Generative AI>

- The Personal Information Protection Commission (PPC) has issued the "Alert Regarding the Use of Generative AI Services and Other Matters" dated June 2, 2023, as well as an alert to OpenAI, L.L.C. and OpenAI OpCo, LLC, which develop and provide ChatGPT, a generative AI service, and has issued the and published the "Summary of Alerts to OpenAI."

II-2. PPC's Alerts against OpenAI

<Alerts, etc., regarding the use of Generative AI Services>

- (i) Business operators handling personal information, (ii) administrative agencies, etc., and (II) general users are reminded to be careful when using the service.

II-2. PPC's Alerts against OpenAI

<Alerts, etc., regarding the use of Generative AI Services>

- Regarding (i) and (ii), we point out the following situations.

When entering a prompt that contains personal information (related to regulations on the purpose of use)

When prompts containing personal data are entered and such personal data are handled for purposes other than outputting the results of responses to such prompts (related to regulations on provision to third parties)

II-2. PPC's Alerts against OpenAI

<Alerts, etc., regarding the use of Generative AI Services.>

- The following risks are noted for (II).
 - The risk that personal information entered into the system will be used for machine learning by generative AI.
 - The risk of inaccurate or incorrect content being output from the Generative AI service.
 - The risk of inaccurate personal information being included in the results of responses to prompts entered.

II-2. PPC's alerts against OpenAI

<Summary of Alerts to OpenAI>

- The "Summary of Alerts to OpenAI" notes the following concerns
- (1) Regulations on acquisition of personal information requiring special consideration (Article 20, Paragraph 2 of the Act on the Protection of Personal Information)

The following four points were made regarding the collection of information for machine learning.

- (i) Necessary efforts shall be made to ensure that the information to be collected does not include any personal information requiring special consideration.

II-2. PPC's alerts against OpenAI

<Summary of Alerts to OpenAI>

- (ii) As soon as possible after the collection of information, measures shall be taken to reduce as much as possible the personal information requiring special consideration that may be included in the collected information.
- (iii) If it is discovered that the collected information contains personal information requiring special consideration even after taking the measures described in (i) and (ii) above, measures shall be taken to delete such personal information requiring special consideration or to make it impossible to identify specific individuals, as soon as possible and before processing it into a data set for learning purposes.

II-2. PPC's alerts against OpenAI

<Summary of Alerts to OpenAI>

- (iv) If the individual or the Personal Information Protection Commission, etc. requests or instructs the Company not to collect the Sensitive Personal Information from a specific site or third party, the Company shall comply with such request or instruction unless there is a justifiable reason for refusal.

If the user selects not to be used for machine learning when entering Sensitive Personal Information into the prompts, the Company shall not handle such information for machine learning, unless there is a justifiable reason for not doing so.

II-2. PPC's alerts against OpenAI

<Summary of Alerts to OpenAI>

(2) Notification of purpose of use, etc.

Notification or public announcement of the purpose of use of personal information regarding both the user and individuals other than the user as the principal, using the Japanese language.

III-1. Privacy concerns in the Metaverse

<Guidelines related to the Metaverse>

- The government's report on the various issues on the Metaverse
- The government's report on the safety in the Metaverse

III-1. Privacy concerns in the Metaverse

<Eye-tracking>

- The eye movements of VR goggle wearers can be used for efficient marketing in the metaverse.
- This is considered more efficient than using cameras to analyse the movements of buyers in front of product shelves in convenience stores.

III-1. Privacy concerns in the Metaverse

<Logging of metaverse participants' behaviour history and ensuring security of metaverse participants. >

- In order to resolve problems in the metaverse between metaverse participants, it is useful to obtain and keep records of logs of the metaverse participants' behaviour history in the metaverse.

III-1. Privacy concerns in the Metaverse

<Monitoring>

- Some metaverses have a VR SNS aspect.
- Some Japanese SNSs check for problems with messages between participants, especially in terms of child protection.
- Telecommunication Business Act
- Anti-Dating Law

III-2. Privacy concerns related to the avatar

<Relationship between the person (inside) and the avatar>

- When one person wears one avatar (one-off, ongoing)
- When one person wears more than one avatar at the same time
- When several individuals wear a single avatar (simultaneously or in shifts).

III-2. Privacy concerns related to the avatar

<Relationship between the avatar's origins and his/her (the person in it) appearance. >

- Patterns for creating avatars based on the appearance of the person in the real world.
- Pattern of creating an avatar that is disconnected from the person's appearance in the real world.

III-2. Privacy concerns related to the avatar

<The person's (inside person's) attitudes towards the avatar. >

- The view of an avatar as an extension of a person's own existence in the real world.
- The view of Avatar as an entity separate from the person themselves in the real world.
- Effects of distance between the metaverse and the real world.

III-2. Privacy concerns related to the avatar

<Situations where the relationship between the person (inside) and the avatar is important. >

- infringement of privacy
- Defamation against the avatar (defamation and violation of honour and sentiment)
- Avatar impersonation.

III-2. Privacy concerns related to the avatar

<Situations where the relationship between the person (inside) and the avatar is important. >

- Unauthorised use of avatar 'likeness'.
- Unauthorised 'portraits' of avatars.

Thank you for your attention!



Special Counsel

**Takashi
Nakazaki**

- Professional Admissions: Japan (2001)
Takashi Nakazaki advises on an extensive range of TMT matters, including telecom regulations, computers, software development, e-commerce, platform service, domain name disputes, and digital forensics. His experience also includes legal advice in several fields of intellectual property and licensing, including traditional copyright, digital copyright, trademark, open source, cross-border licensing and biochemicals. He has also assisted many start-up clients with general corporate advice.

E-mail: takashi.nakazaki_grp@amt-law.com
Tel: 81-3-6775-1086

Education

- The University of Tokyo (LL.B., 1998)
- Graduate study, Columbia University School of Law (LL.M., 2008)
- Associated with Arnold & Porter LLP, September 2008 - June 2009

Professional and Academic Associations

- Associations and Committees Liaison Officer, Technology Committee, IBA
- Member, Task force on Drafting New AI Guidelines for Business, for the Ministry of Economy, Trade and Industry (METI), Government of Japan
- Member, Public-Private Partnership Council on Addressing New Legal Issues Concerning Content in the Metaverse, Cabinet Office, Government of Japan
- Member, Expert Study Committee on the Rules of AI Governance and Management of the Study, for the Ministry of Economy, Trade and Industry (METI), Government of Japan
- Member, Working Group on the Creation of a Safe and Secure Environment for the Use of Smartphones in the Smartphone Era, for the Ministry of Internal Affairs and Communications, Government of Japan
- Member, Working Group on Omotenashi Platform to Promote Consumption by Foreign Tourists, for METI, Government of Japan
- Member, Working Group to Promote the Dissemination of IoT (Internet of Things) Data, for METI, Government of Japan
- Co-founder, IAPP (International Association of Privacy Professionals) Knowledge Net Tokyo
- Editor, International Association for the Protection of Intellectual Property of Japan