

Client Alert

28 July 2022

**For further information
please contact:**



Kensaku Takase
Partner
03 6271 9752
Kensaku.Takase@bakermckenzie.com



Daisuke Tatsuno
Partner
03 6271 9479
Daisuke.Tatsuno@bakermckenzie.com



Tsugihiko Okada
Counsel
03 6271 9541
Tsugihiko.Okada@bakermckenzie.com



Juna Suekane
Associate
03 6271 9743
Juna.Suekane@bakermckenzie.com

Personal Information Protection Commission releases its annual report

In June 2022, the Personal Information Protection Commission (PPC), which is the regulatory authority for the protection of personal information in Japan, published its 2021 annual report ("Report"). While the Report does not supplement the law in any way, it does provide businesses with useful insights on the PPC's thinking and position with respect to various types of processing of personal information under Japanese law.

The PPC's activities for smooth implementation of amendments to the APPI

The main part of the Report starts with an introduction of the PPC's efforts undertaken over the past year towards assisting with the implementation of the amendments to Japan's privacy law (the Act on the Protection of Personal Information (APPI)) that came into effect on 1 April 2022.

The amendments to the APPI introduced several new rules, which had a practical impact on businesses, including the following:

- Strengthened requirements for cross-border transfers of personal data
- Mandatory reporting of data breach incidents
- Restriction on the transfer of "Personally Referable Information"
- Introduction of new rules on processing pseudonymized information

The PPC's activities in relation to these amendments include its release of updated guidelines. In addition, regarding the new requirements for cross-border transfers of personal data, the PPC published a report on the key differences between the privacy laws of 31 jurisdictions and Japan. While being detailed and somewhat difficult at times to put into practice, the materials attempt to provide practical guidance to businesses.

Warning for processing of personal data in relation to business succession and the operation of e-commerce sites

According to the Report, there were 5846 data breaches involving the leakage of personal data reported to the PPC from 1 April 2021 to 31 March 2022. While the majority (54.9%) of the cases were caused by erroneously sending documents and emails or losing documents and electronic media, notably, the number of incidents caused by unauthorized access amounted to 24.4%, an increase from 17.8% in the same period in the previous year. This shows that the number of data leakage incidents caused by unauthorized access or cyberattacks in Japan is increasing like in many other jurisdictions. This indicates the importance for businesses to implement cybersecurity and other appropriate security measures to protect personal data.

In addition, the Report particularly highlights the improper handling of personal data in relation to business succession (such as M&A) and the operation of e-commerce sites.

Japanese privacy law is primarily based on giving notice to data subjects, rather than requesting consent. For business succession, the Report points out that the PPC observed unlawful processing of personal data where a successor business operator used personal data beyond the scope of the purpose of use notified or made available to the data subjects. Such an excessive use of personal data is expressly prohibited by the APPI. The Report emphasizes that successor companies need to make sure that there are no unlawful changes in the scope of use of personal data.

For the operation of e-commerce sites, the Report points out that there were many cases of unauthorized access to customer personal data. Unauthorized access to an e-commerce site causes serious concern because e-commerce sites often hold credit card information or other payment information, which may have a material adverse impact on data subjects. It is advisable for e-commerce sites to review their security practices, considering the increase of unauthorized access to e-commerce sites and the PPC's observations. Cybersecurity is also a key theme that arises again here.

Pseudonymized information and anonymized information

The Report introduces the PPC's release of an updated version of the report concerning pseudonymized information and anonymized information on 30 March 2022. The report was released to give guidance related to the pseudonymized information system established by the amendments to the APPI on 1 April 2022. In the report, the PPC provides guidance for the creation and use of pseudonymized information and examples of proper use of pseudonymized information.

Anonymized information allows businesses to use big data, particularly for advertising, statistics or marketing activities. According to the Report, the PPC is aware of 664 companies that have publicly announced that they are effectively using the anonymized information system in business as of 31 March 2022. Because the use of data for business (e.g., utilization of real-world data in the medical industry) is attracting more and more attention, it is expected that an increasing number of businesses will use the anonymized information in a near future.

Supervision based on the APPI

According to the Report, as part of the PPC's supervision over processing of personal information, it took the following number of enforcement actions in 2021:

- Acceptance of reports on cases of data breach incidents: 1042
- Report orders: 328
- Guidance and advice: 217
- Recommendations: 3
- Cease and desist orders: 1

The cease and desist order was issued to a business operator who illegally publicized the personal data of many persons who faced bankruptcy on its website. Prior to issuing the order, the PPC issued a recommendation to the

business operator, but no measures related to the recommendations were taken. The order required the business operator to stop publicizing personal data on its website.

While the number of enforcement actions may appear limited, the fact that the PPC issued the cease and desist order shows that it is willing to enforce the APPI, particularly where it considers there to be serious violations.