# The top three data protection law topics in Japan

Saori Hanada, partner, Fumiaki Matsuoka, partner, and Osamu Fujiwara, partner, Atsumi & Sakai

**Saori Hanada**
Partner, Atsumi & Sakai
saori.hanada@aplaw.jp

**Fumiaki Matsuoka**
Partner, Atsumi & Sakai
fumiaki.matsuoka@aplaw.jp

**Osamu Fujiwara**
Partner, Atsumi & Sakai
osamu.fujiwara@aplaw.jp

In Japan, the Act on the Protection of Personal Information (APPI) is the primary law that regulates data protection issues. In this article, we will cover a few significant recent amendments to the APPI, including one currently under consideration, while also touching on the new guidelines issued by the Japan Fair Trade Commission (JFTC) last year, which highlight an intersection of the APPI and Japanese competition law, as well as the increasing significance of personal data in M&A transactions.

## 2015 amendments to the APPI

The APPI was enacted in 2003 and went through its first major amendment in 2015 (the 2015 amendment). In accordance with the 2015 amendment, the Personal Information Protection Commission (PPC) was established as the supervisory governmental organisation for privacy protection on 1 January 2016, and since then the agency has issued a number of administrative guidelines concerning the APPI. The 2015 amendment was fully enforced in 2017, which led to another noteworthy development with regard to the APPI. The European Commission (EC) recognised the APPI as having an adequate level of data protection by GDPR standards in 2019. This adequacy decision by EC was met with open arms by Japanese companies as it would allow for data transfers from EEA to Japan without additional safeguard measures.

## 2020 Amendment to the APPI

On 10 March 2020, the cabinet submitted a bill to amend the APPI which is expected to be enacted into law in 2020 (the 2020 amendment).

Companies will face more stringent obligations under the 2020 amendment. For example, while the current APPI does not stipulate any reporting obligation on data breach, there will be a legal obligation to report certain data breaches after the reform. The penalties for violating orders issued by the PPC will also be harsher. In its preparation for the 2020 amendment, the PPC, being the agency in charge of this amendment, looked to the GDPR for guidance as it viewed the GDPR as the global standard for data protection, and it was important for the APPI to have an adequate level of data protections by the GDPR standard.

Although companies outside of Japan will be required to be compliant with APPI after the enforcement of the amendment, there are currently a substantial number of cases where companies outside of Japan do not appropriately process personal information of individuals within the country. Companies, including those non-compliant companies, will definitely need to promptly report to the PPC in the event of data breach taking place outside of Japan. This is because, after the amendment, the PPC will be issuing orders to companies abroad that process personal data of individuals in Japan inappropriately, and will publish those cases on its website.

> **The Guidelines provide a non-exhaustive list of conducts by digital platform operators related to the use of personal information which can amount to an abuse of superior bargaining position.**

**Digital platform operators and personal information**

The JFTC, the primary enforcement agency of the Antimonopoly Act, the main competition law in Japan, published the *Guidelines Concerning Abuse of a Superior Bargaining Position in Transaction between Digital Platform Operators and Consumers that Provide Personal Information etc* (the Guidelines) on 17 December 2019. An 'abuse of a superior bargaining position' is a unilateral conduct prohibited under the Antimonopoly Act, which is analogous to an abuse of dominance. For business operators to be held accountable for the abuse of a superior bargaining position, there needs to be a comparatively superior position vis-à-vis a business operator's counterpart in the transactions between them, not dominance in the market.

With the aim to clarify and enhance the predictability for digital platform operators as to the enforcement of the Antimonopoly Act, the Guidelines provide a non-exhaustive list of conducts by digital platform operators related to the acquisition or use of personal information which can amount to an abuse of superior bargaining position. Such conducts include acquiring personal information without stating the purpose of use to consumers, acquiring or using personal information against consumers' intention beyond the scope necessary to achieve said purpose of use, and acquiring or using personal data without taking necessary and appropriate precautions for the safe management of personal information.

As the Guidelines concern issues regulated by the APPI, the PPC issued a statement saying that it would co-operate with the JFTC when it discovers facts that can potentially be deemed as an unfair acquisition or use of personal information by a digital platform operator which holds a superior bargaining position. In return, the PPC requested the JFTC to co-operate when it discovers a potential abuse of a superior bargaining position related to the treatment of personal information so that the PPC can evaluate the relevant facts from its perspective. In response, the JFTC agreed to co-operate with the PPC on the abuse of a superior bargaining position between digital platform operators and consumers providing personal information to the extent necessary.

**Data compliance in M&A deals**

The Information Commissioner's Office (ICO), the supervisory authority in the UK, announced its intention to impose a fine of more than £99,200,396 on Marriott International, Inc for its infringements of GDPR last year. It was also revealed by the ICO that Marriott failed to conduct sufficient due diligence in its acquisition of Starwood.

In Japan, this case drew significant attention as Marriott was found to be responsible for the vulnerability of Starwood's IT system in a cybersecurity incident which took place prior to the acquisition. Through this case, Japanese companies reaffirmed the importance of compliance with personal data protection laws in M&A transactions. In particular, as a purchaser, companies must emphasise the importance of due diligence focused on data protection (DDDP) of their target companies in M&A transactions. The results of DDDP should then be used by the purchasers for not only deciding whether or not to proceed with the M&A transaction and examining the validity of purchase prices but also for establishing action plans to properly process personal information of their target companies post-closing. It is also advisable for the purchasers to consider inserting into their M&A agreements essential clauses such as representations and warranties as well as covenants in order to hedge the risks related to data protection. In practice, however, purchasers cannot always conduct a full DDDP for various reasons such as sellers refusing to disclose all the necessary information about them, the purchasers being unable to bear costs of the DDDP etc. It is therefore advisable for Japanese companies to determine the scope of their DDDP, by prioritising in each individual transaction. ■