Personal Information Protection Commission – recent trends

24 January 2020 | Contributed by Nagashima Ohno & Tsunematsu

AUTHORS

Oki Mori

Takiko Kadono

In recent months, the Personal Information Protection Commission (PPC) has been proactive in publicising cases of data breaches that have had a significant social impact, together with the names of the companies.

Background

With the partial enforcement of the amended Act on the Protection of Personal Information in January 2016, the PPC was established as a regulatory body responsible for managing and ensuring compliance with the act. Under the act, the PPC has been granted supervisory authority over companies that were previously regulated by the relevant competent ministers. Specifically, the PPC is empowered to issue:

- formal requests to report, conduct onsite inspections and issue formal guidance (*shidou*) and advice (*jogen*) to companies to the extent necessary for the enforcement of the act; and
- formal recommendations (*kankoku*) or orders (*meirei*) to companies when they violate certain provisions and requirements of the act.

The PPC's establishment has significantly increased the supervisory authority's work at large.(1) On the other hand, until recently, it was common practice for the PPC not to publicise the names of companies that were subject to PPC investigations or orders. In fact, until July 2019, the PPC had publicised only one case where it identified the relevant company by name.(2)

Recently publicised cases

From August to December 2019, the PPC publicised the details of three data breach cases, together with the names of the relevant companies.

Case one

On 26 August 2019, together with the name of the relevant company, the PPC publicised the fact that it had issued a formal recommendation and guidance to a major Japanese human resources service company that operates a job hunting website (Company X). The PPC found that Company X had:

- provided the personal data of approximately 8,000 job hunting students who were members of its website to its client companies without obtaining the consent of the data subjects; and
- failed to take necessary and appropriate measures for the secure management of personal data.

In its recommendation and guidance, the PPC instructed Company X, among other things, to:

- improve its awareness of the protection of personal data on a company-wide basis;
- ensure that personal data is handled appropriately in accordance with the Act on the Protection of Personal Information when designing and operating new services; and
- provide clear information for data subjects to determine whether to agree to their personal data being provided to third parties.

The PPC stated that it had publicised the case in light of its social impact.

Further, on 4 December 2019, together with the names of the relevant companies, the PPC publicised that it had issued:

- a formal recommendation and guidance to Company X for a second time;
- a formal recommendation to a company that outsources work to Company X; and
- formal guidance to 37 client companies of Company X that had used its services.(3)

An investigation conducted after the first recommendation had been issued to Company X revealed new facts concerning violations of the Act on the Protection of Personal Information, which increased the number of data subjects affected by the data breach to approximately 26,000. In the recommendations and guidance, the PPC instructed:

- Company X, among other things, to establish a system to ensure that personal data is handled appropriately in accordance with the act when designing new services;
- the outsourcing company to conduct necessary and appropriate supervision over subcontractors when outsourcing work; and
- the client companies, among other things, to notify or announce the purpose of their use of personal data appropriately and, in certain cases, to conduct an organisation-wide legal review and take necessary action when providing personal data to third parties.

Case two

On 17 September 2019, together with the name of the relevant company, the PPC publicised the fact that it had issued formal guidance twice to a Japanese company that provides taxi-related services (a taxi dispatch application). The PPC found that the company had not sufficiently informed taxi users that it would capture their facial images with a camera attached to a tablet terminal installed in its taxis and use the images to optimise advertising distribution. Although the PPC issued guidance to the company in November 2018 and instructed it to provide a simplified explanation to taxi users, the company did not implement improvement measures until April 2019. In light of the above circumstances, the PPC issued guidance for a second time and publicised the case together with the name of the company in September 2019.

Case three

On 11 October 2019 the PPC publicised the fact that the personal data (eg, name, delivery address and order history) of approximately 110,000 user accounts on an e-commerce website operated by a major online retailer headquartered in a foreign country may have been viewable by other users due to a temporary system error. While the PPC instructed the company to take measures to prevent a recurrence of the data breach and to respond to inquiries from the users, it did not exercise supervisory authority over the company pursuant to the Act on the Protection of Personal Information.

Comment

As described above, the PPC has been proactive in publicising cases of data breaches that have had a significant social impact, even when the PPC did not exercise its supervisory authority over the companies in question. Whether this trend will continue should be carefully monitored.

The PPC's views in the above three cases also provide the following practical reference points for companies:

- In the first case, the PPC pointed out that there was a procedural mistake when Company X changed its service and amended its privacy policy. As a result, Company X provided the personal data of members who had registered prior to the service change to the third party without obtaining their consent. This suggests that when companies change their service and amend their privacy policy, they should carefully consider whether they are doing so in accordance with the procedures required by the Act on the Protection of Personal Information (eg, whether they need to obtain consent from existing users).
- In the first case, the PPC found that Company X had not appropriately considered compliance with the act when providing the service in question and had no system to prevent, detect or correct any procedural deficiencies. This suggests that companies must establish a system capable of protecting personal data, including detecting and correcting any identified deficiencies. Companies must also sufficiently consider whether they are structured to comply with the requirements of the act when they commence the provision of new services.
- In more than one case, the PPC mentioned that privacy policies and/or the explanations of how companies handle personal data were difficult for users to understand. The PPC is expected to continue to closely review whether privacy policies and/or explanations to data subjects are appropriate and easily understandable.

For further information on this topic please contact Oki Mori or Takiko Kadono at Nagashima Ohno & Tsunematsu by telephone (+81 3 6889 7000) or email (oki_mori@noandt.com or takiko_kadono@noandt.com). The Nagashima Ohno & Tsunematsu website can be accessed at www.noandt.com.

Endnotes

(1) For example, there were less than 10 formal requests to report per year prior to the PPC's establishment in 2016. However, the PPC issued 305 formal requests to report in fiscal year 2017 and 391 in fiscal year 2018. On the other hand, no more than one recommendation has been issued per year in the past few years, and no orders have been issued thus far.

(2) On 22 October 2018, together with the name of the relevant company, the PPC publicised the fact that it had issued formal guidance to a major social networking service company headquartered in a foreign country. According to the PPC:

- the company had inappropriately received personal data such as website browsing history;
- the company had inappropriately provided its users' personal data obtained through an application to a third party; and
- users' data had been accessed without authorisation by a third party.

In the guidance, the PPC instructed the company, among other things, to provide a simplified explanation to its users and to make sure to thoroughly monitor the status of application activities on its platform. The PPC said that it publicised the case in light of its social impact.

(3) However, with respect to the formal guidance issued to 37 client companies of Company X that had used its services, the PPC did not publicise the names of three companies that had not purchased the personal data in question.
