AMENDMENTS TO THE PROTECTION OF PERSONAL INFORMATION ACT OF JAPAN

The protection of personal data has been an area of increasing focus in Japan in recent years following a series of high profile data breaches. The most recent amendment (the Amendment) establishes a reporting obligation in the event of a data breach, provides stronger rights to data subjects and introduces restrictions on the provision of cookies to third parties. As the Japanese regulator will be able to require foreign companies to report how personal data is being managed, both Japanese and foreign companies should consider how their privacy policies may need to be amended in relation to the use and protection of personal data in Japan.

Key issues

- The Amendment is aimed at establishing an obligation to report data breaches to the PPC and to notify data subjects affected.
- Data subjects will have broader rights with respect to the management of their personal data.
- Cookies are not considered as personal information under Japanese law, however, the transfer of cookies to a third party will be restricted if such third party may identify the individual from such cookies.
- The Amendment extends the extraterritorial scope of the PPC's authority, allowing the PPC to require foreign companies to submit certain information to the PPC.
- The Amendment also seeks to increase penalties against organisations for violations of PPC orders and place restrictions on personal data transfers to third parties outside Japan.

BACKGROUND

The Act on the Protection of Personal Information (APPI) was passed in 2003 and primarily relates to data privacy and the protection of personal data in Japan. In 2017, the APPI was substantially amended, with one of the key changes being the introduction of the Personal Information Protection Commission (PPC), an independent agency with a focus on protecting personal data of individuals in Japan.

The PPC's core focus is promoting a balance between the protection of personal data and the effective use of personal data, particularly in light of increasing technological innovation, and responding to new risks associated with the increasing frequency of cross-border data transfers.

RECRUIT

In August 2019, the PPC determined that Recruit Career (Recruit), which is the operator of the "Rikunavi" job information website, one of the largest recruitment websites in Japan, violated the APPI by selling data to companies which allowed those companies to determine the likelihood of job-hunting students declining job offers.

Recruit used "cookies" in order to track and collect users' web browsing history, and artificial intelligence to analyse the records of students browsing through its website, without obtaining the consent of the students. Recruit then sold the harvested data to about different 40 companies. The PPC concluded that Recruit's sale of the data, without obtaining the users' consent, constituted a violation of the APPI and issued an administrative admonishment (the first of its kind issued by the PPC). The admonishment required Recruit to review its organisational structure and review the awareness of its staff on the issue of

the protection of data, handle personal information properly in future services it offers and provide an explanation to its users who had agreed to provide their personal data on how that data would be used.

Driven partially by the handling of personal data by large corporates such as Recruit, the Japanese government plans to further revise the APPI by introducing new provisions designed to increase the rights of individual data subjects and aimed at preventing companies from mis-using personal information (the Amended APPI). The Amended APPI was enacted on 5 June 2020 and is likely to come into force from spring 2022.

AMENDMENTS

The key changes made by the Amendment are summarised below.

(i) **Increased data subject rights**

- Under the current APPI, a private business operator handling personal information (an Operator) is not required to cease using, or to delete, personal data upon any request of the data subject. A data subject can only require the Operator to do so if:

  (a) the personal data was used for a purpose other than the purpose originally notified;

  (b) it was published; or

  (c) it was collected in an illegal manner.

  This will change under the Amended APPI: the data subject can also request that their personal data is deleted if the personal data is inappropriately used, if the Operator no longer needs to use the information, or if the relevant data is accidently leaked.

- Increased digitalisation – data subjects will be able to require that the data held on them by an Operator is provided to them in electronic format. The current APPI does not provide for electronic disclosure and disclosure requirements are met through the disclosure of hard copy documents. 'Short term' data, which under the current APPI means data that is prearranged to be erased within 6 months from its acquisition, will also have to be disclosed – all personal data will therefore qualify as retained personal data regardless of the retention period.

- Under the current APPI, personal data can be provided to third parties without consent if data subjects are given the right to "opt out". The Amended APPI will limit the scope of personal data that can be provided based on this "opt out" exception.

- Under the Amended APPI, a data subject will also be entitled to request that an Operator discloses records setting out the personal data that has been disclosed by the Operator to any third parties.

(ii) **Increasing responsibility on Operators**

Under the current APPI, an Operator is only required to "make an effort" to submit a data breach report to the PPC if there is a loss of personal data, and it is only recommended that the Operator notifies data subjects (it is not mandatory for the Operator to do so). The Amended APPI creates a new obligation on Operators to notify the PPC and the applicable data subject in the event of a data breach. According to the PPC, it is also designed to make clear that companies cannot use personal data in an "improper manner" – the guidance produced by the

PPC on what may constitute an "improper manner" refers to the use of personal data "that may not necessarily be illegal under the current APPI, but that cannot be overlooked in terms of protecting individual rights and interests, such as using personal information in ways that may potentially facilitate or induce illegal or unjustifiable conduct".

(iii) **Cookies**

- The Amended APPI will also require: (a) businesses that obtain and use information collected through the use of third party cookies, such as cookies provided by data management platform (DMP) vendors, to obtain the consent of internet users before doing so; and (b) DMP vendors to confirm whether the consent of internet users has been obtained when these cookies are provided to third parties.
- Cookies are not considered personal data under the current APPI, on the basis that a cookie does not include information which can identify an individual user. However, when cookies are combined with other information, they may be used to identify individuals.
- The Amended APPI aims to address this gap in the law by introducing the concept of "personally identifiable information" (*kojin kanren jyoho*), which means information that does not constitute personal data when held by a data transferor (e.g., a DMP vendor) but is capable of identifying a specific data subject when it is collated with other information by a data transferee (e.g., a company using cookie data). This will also be treated as personal information.
- Measures that can be taken by businesses that obtain "personally identifiable information" through third party cookies will be introduced to help mitigate the risks associated with cookies, and will include:

  (a) businesses being required to specify and disclose information about cookies on their privacy policies or cookie policies;

  (b) a requirement that a business that discloses information to a third party obtains the data subject's consent to do so;

  (c) if a business uses a third party cookie, the business must disclose the name of the cookie issuer and the URL of such issuer's privacy policy; and

  (d) businesses being required to create a system under which they cannot obtain cookie information until the data subject gives its consent to the collection of such information (and the data subject being able to withdraw its consent).

(iv) **Pseudonymised Information**

- In order to enhance the utilisation of personal data, the Amended APPI will also introduce a new category of personal data called "pseudonymised information" (*kamei kakou jyouhou*) (which is a concept that also exists under the General Data Protection Regulation (GDPR)). The "pseudonymisation" of data, being the replacement or deletion of a description that can directly identify a specific individual, will be permitted in some form, with the intention that controls on data that has been pseudonymised will be relaxed; for example, the rights of data subjects to demand disclosure, correction or the cessation of usage of pseudonymised information.

EXTRATERRITORIAL APPLICABILITY

Currently, the PPC does not have the authority to require foreign companies that handle personal information, or anonymously process information produced by using personal information related to a data subject in Japan, to submit information on how that data is being managed. The Amended APPI will extend the extraterritorial scope of the PPC to allow the PPC to do so and to publish the fact that an overseas company did not follow a PPC order.

The Amended APPI will also strengthen existing regulations related to the transfer of data to third parties outside of Japan.

Currently, a cross-border transfer of personal data generally requires the prior consent of the data subject, unless: (i) the transferee (the third party receiving the data) is located in a country that the PPC considers to have a level of data protection equivalent to that of Japan (which included, as of the date of this briefing, the countries in the European Economic Area); or (ii) the transferee has established the same standard of protection as required under the APPI (e.g., the transferor enters into an appropriate data transfer agreement with the transferee or, if the transferee is an affiliate of the transferor, the transferor has established an appropriate global privacy policy which applies both to the transferor and the transferee).

Under the Amended APPI, if personal data is provided to a third party outside of Japan on the basis of the consent of a data subject, the Operator in Japan is required to provide the relevant data subject with information in respect of how the third party recipient handles such data, including the names of the countries that the data is exported to and information relating to whether there are regulations to protect personal data in those countries.

PENALTIES

The Amended APPI will also amend the penalty regime in Japan, in line with the global trend of strengthening data privacy penalty regimes. The Amended APPI will impose:

- 1 year imprisonment or a fine of up to JPY 1 million for a breach of a reporting order by the PPC; and
- more severe penalties on legal entities compared to natural persons – fines imposed by the PPC on legal entities will be up to JPY 0.1 billion.

IMPACT ON YOUR BUSINESS

We expect that the Amended APPI will have a major impact on businesses that operate in Japan and the way they handle personal data. Businesses may need to update their privacy policies and ensure their data handling rules and operations are in compliance with the Amended APPI. It would be also advisable for companies to establish an internal protocol in case of a data breach, together with the protocol for other applicable legal regimes such as the GDPR. Given the extraterritorial applicability of the regulations, we expect many foreign companies and organisations will also be affected.

Japanese and foreign companies should therefore seek professional advice, particularly given that the scope and applicability of the new regulations are broadly defined, and as a result of the increasing focus of the PPC and other Japanese regulators on data protection and privacy issues in light of the Recruit case and other high profile data breaches.

COMPARISON WITH EU REGULATIONS

The changes made by the Amended APPI bring Japan's data protection regime closer in alignment with the EU Regulations (comprising the GDPR and, in relation to cookies, the ePrivacy Directive). The table below shows the key similarities and differences between the Amended APPI and the EU Regulations. It is notable that under the GDPR there is a duty to report notifiable data breaches to the supervising authority within 72 hours of becoming aware of the breach, and the financial penalties for non-compliance with the GDPR remain much higher than the Amended APPI.

	Amended APPI	EU Regulations
Data subject rights of erasure, data portability and access to personal data	✓	✓
Obligation to notify individuals affected by a data breach	✓	✓
Set timeframe to report data breach	Promptly following the data breach	72 hours
Legitimising cross border transfers of personal data	Prior consent of the data subject is required Recipient country has the equivalent level of protection to that of Japan Transferee applies the same standard of protection as required under the APPI contractually	Recipient country has adequate protection EU standard contractual clauses Binding corporate rules
Extra-territorial applicability	✓	✓
Consent required for cookies	✓ (where "personally identifiable information" is obtained)	✓ (except where the cookies are "strictly necessary")
Relaxed rules for pseudonymised information	✓	✓
Penalties for non-compliance	1 year imprisonment or a fine of up to JPY 1 million or for more serious breaches by legal entities up to JPY 0.1 billion	€10m or 2% of global turnover for lower level breaches €20m or 4% of global turnover for serious breaches

CONTACTS

Natsuko Sugihara
Partner

T +81 3 6632 6681
E natsuko.sugihara
@cliffordchance.com

Tatsuhiko Kamiyama
Partner

T +81 3 6632 6395
E tatsuhiko.kamiyama
@cliffordchance.com

Michihiro Nishi
Partner

T +81 3 6632 6622
E michihiro.nishi
@cliffordchance.com

Masafumi Shikakura
Counsel

T +81 3 6632 6323
E masafumi.shikakura
@cliffordchance.com

Timothy Merchant
Senior Associate

T +81 3 6632 6631
E timothy.merchant
@cliffordchance.com

Hitomi Kurokawa
Senior Associate

T +81 3 6632 6632
E hitomi.kurokawa
@cliffordchance.com

EU Regulations

Luke Grubb
Partner

T +65 6506 2780
E luke.grubb
@cliffordchance.com

Antonia Anderson
Associate

T +65 6506 2750
E antonia.anderson
@cliffordchance.com

www.cliffordchance.com

Clifford Chance (Gaikokuho Kyodo Jigyo)

Palace Building, 3rd floor

1-1, Marunouchi 1-chome, Chiyoda-ku, Tokyo 100-0005, Japan