Newsletter

ATSUMI & SAKAI
TOKYO | NEW YORK | LONDON | FRANKFURT
www.aplaw.jp

▶ About us

Atsumi & Sakai is a multi-award-winning, independent Tokyo law firm. The firm operates as a foreign law joint venture, combining a comprehensive Japanese-law practice with a team of foreign partners and lawyers from major international law firms to provide its clients with the benefit of both Japanese law expertise and real international experience. Expanding from its highly regarded finance practice, the firm now acts for a wide range of international and domestic companies, banks, financial institutions and other businesses.

Amendments to the Act on the Protection of Personal Information

October 2021 A&S(EN)_011

Introduction

With the rapid advance of digitalization, companies are now processing personal information outside of Japan. However, many users are not aware that their personal information collected in connection with these services is processed outside of Japan. There are also cases where companies providing such services are not apprised in relation to processing of data under foreign data processing systems or through other foreign companies.

To protect the rights and interests of individuals, the Act on the Protection of Personal Information of Japan ("APPI"), as well as privacy laws in other countries, such as the GDPR in the EU, are becoming stricter. Under these stricter privacy laws, mere explanations by companies about how they handle data, alone, are now considered insufficient, and by extension, services provided by such companies could be considered unacceptable from a data protection perspective.

In Japan, companies are now required to give more in-depth explanations as to how they gather and process personal data, as well as the protection measures and systems in place. In order to properly explain how personal information is transferred and handled outside of Japan, it is necessary for such companies to have an understanding of the data protection and privacy laws of other countries (e.g., the GDPR), and to be apprised of the data handling status of foreign companies.

To meet this new challenge, it is important to understand the guidelines of the Personal Information Protection Commission ("PPC"), and in order to communicate effectively with overseas companies, it is necessary to be aware of the differences between the provisions of the GDPR and APPI. However, it is not possible to address this issue by simply providing an overview of the APPI. Therefore, in this newsletter series, we will present the views of former PPC member, Haruhi Kumazawa, as well analysis from our Frankfurt Office.

Question:

I am responsible for compliance with the APPI at my company. Under the APPI Amendment Act of 2020, it is now necessary to consider measures that need to be implemented, as well as the schedule. What is the schedule and contents of the Amended Act of 2020?

Contents of Answer:

1. Schedule of the 2020 Amendment of the APPI (the "Amendment Act") - From Promulgation to Enforcement

The following table details the schedule of the Amendment Act of 2020, from promulgation to enforcement.

Jun 12, 2020	Promulgation of the 2020 Amendment Act
Mar 24, 2021	Promulgation of revised administrative rules based on the 2020 Amendment Act
May 19, 202	Promulgation of the 2021 Amendment Act[1]
Aug 2, 2021	Release of revised guidelines based on the 2020 Amendment Act by PPC
Sep 10, 2021	Release of revised Q&A based on the 2020 Amendment Act by PPC
Apr 1, 2022	Enforcement of the 2020 Amendment Act

Companies have to be in complete compliance with the 2020 Amendment by the enforcement date, which is April 1, 2022.

---

[1] The purpose of the 2021 Amendment is to revise the rules applied to the Japanese public sector.

2. Material Revisions in Practice

Although various revisions have been made, the following matters are those of which we are frequently consulted. (The details will be explained below from Section 3 onwards.)

(1) Obligations related to the transfer of personal data outside of Japan: where a company causes personal data to be transferred outside of Japan, it is now necessary, pursuant to the Amendment Act, to explain matters such as the systems concerning the protection of personal information in such foreign country (Article 24, paragraphs 2 and 3 of the Amendment Act).

(2) New concept: Personally referable information: to address services using information from which, by itself, it is difficult to identify individuals, such as internet browsing history, location information, and cookies, the Amendment Act introduces the concept of "personally referable information" and stipulates an obligation to obtain consent in certain cases (Article 26-2 of the Amendment Act).

(3) Obligations in the event of a personal data breach: the Amendment Act stipulates an obligation to report personal data breaches to the Personal Information Protection Commission and to notify the data subject concerned (Article 22-2 of the Amendment Act).

It appears that even prior to the amendment to the APPI, many Japanese companies have had internal regulations that require the making of incident reports, reporting to the Personal Information Protection Commission and notification to the data subjects. It will be necessary to consider the Personal Information Protection Commission's guidelines, etc., and review current internal regulations and contracts before the Amendment Act comes into effect.

(4) New concept for APPI: "Pseudonymously processed information" : under the Amendment Act, new rules have been introduced regarding "pseudonymously processed information", i.e., information without names, etc., per Article 2, paragraphs 9 and 10, Article 35-2, and Article 35-3 of the Amendment Act. This category of information is easier for companies to use than "anonymously processed information", and there are less obligations imposed on a company that only handles "pseudonymously processed information".

It is anticipated that pseudonymously processed information will be used for customer analysis and when handling pharmaceutical and medical information in particular.

Comments from the former Personal Information Protection Commission member Haruhi Kumazawa on the Amendment Act

(i) Background to the amendment of the APPI

The purpose of the APPI is to balance the utilization and protection of personal information. This refers to "protecting an individual's rights and interests while considering the utility of personal information" .

The underlying spirit of the APPI is for the promotion of the utilization of personal data, while protecting both the rights and interests of individuals who are data subjects and the rights and interests of individuals to utilize personal data. If a company utilizes personal information without taking adequate protective measures, the rights and interests of individuals are likely to be violated, and the services of that company will, consequently, come under scrutiny. The future utilization of personal information by such company, in such instance, will be restricted. Thus, it is of crucial importance to protect personal information in the interests of utilization. The APPI and GDPR share this fundamental spirit.

The 2015 revision of the APPI includes a provision stipulating that the act be reviewed every three years in the context of the continuing advancement and progress of cross-border information flow. The PPC, an incorporated administrative agency, took charge of this review when the act was amended in 2020.

(ii) PPC's efforts and the 2020 amendment

A number of issues have come to light since the 2015 amendment. From its establishment, the PPC has worked to facilitate the smooth implementation of the reforms through the legal system by, among others, formulating ordinances, rules, and guidelines. At the same time, the PPC has handled cases involving leakage and misuse of personal information, as well as the mediation of complaints from individuals. In addition to the experience gained through these efforts, the PPC has received the opinions of various stakeholders related to personal information, including business groups, consumer groups, academics, and legal experts. Furthermore, the PPC has engaged in dialogue with the EU and the United States, and exchanged information within the existing international frameworks such as the OECD and APEC, as well as with data protection organizations in various jurisdictions. Through these efforts, the PPC has been able to assess the current situation regarding protection of personal information, and identify potential future issues, which has informed and guided the draft, enactment and implementation of the amendment to the APPI to promote

and balance the utilization and protection of personal information.

(iii) A message to people who deal with personal data

The APPI is perceived as having moved in a more conservative direction. However, this Amendment Act will regulate areas of business and situations where companies are at risk of inappropriate handling and utilization of personal information. This Amendment Act will encourage companies to handle and utilize personal information (an important management resource) with transparency and accountability.

As mentioned above, if you do not protect personal information, your company's services may come under scrutiny. Among the opinions we received from various companies, many expressed concern that their services might infringe on the rights and interests of individuals. We hope that companies will see this Amendment Act as an important opportunity to review their own internal processes for handling personal information.

3. Transfer of Personal Data Outside of Japan

(1) Background of establishment of rules on the transfer of personal data outside of Japan

Although the APPI stipulates that, in principle, the data subject's consent must be obtained when providing personal data outside of Japan, prior to the amendment, it was not necessarily required to provide information on the name of the country in which personal data would be stored/processed, or the systems related to the protection of personal information in such country.

On the other hand, as data protection related legislation has become more prevalent throughout the world, the risks associated with cross-border transfers of personal data are changing, such as regulations on state control of personal data in some countries. Some consumers expressed concern that they are not sufficiently informed of how their own personal data is being handled outside of Japan.

The reality that there are differences in data protection systems between jurisdictions raises the issue of foreseeability in relation to individuals and business operators handling personal data, which, understandably, is a cause for concern for data subjects.

It was decided with respect to Article 24 of the Amendment Act, which restricts international data transfer, to require companies to inform/alert data subjects of certain matters, at a minimum, regarding foreign companies, based outside of Japan, to which personal data will be transferred, as well as the robustness of the data protection system in the jurisdiction the foreign company is located in.

(2) Rules on the transfer of personal data outside of Japan

Article 24, paragraphs 2 and 3 of the Amendment Act provide for the transfer of personal data outside of Japan as follows.

Article 24, paragraph 2:

A personal information handling business operator shall, in the case of obtaining a principal's consent pursuant to the provisions of the preceding paragraph, in advance, provide the principal with information on the personal information protection system of the foreign country, on the measures the third party takes for the protection of personal information, and other information (reference purposes), pursuant to the rules of the Personal Information Protection Commission.

Article 24, paragraph 3:

A personal information handling business operator shall, when providing personal data to a third party (limited to a company establishing the appropriate system stipulated by APPI) in a foreign country, pursuant to the rules of the Personal Information Protection Commission, take necessary action to ensure continuous implementation of the equivalent action by the third party, and, in response to a principal's request, provide information on the necessary action to the principal.

Pursuant to the above provisions, when causing personal data to be transferred outside of Japan, it is necessary to provide the information prescribed in the amended administrative rules of the APPI (the "Amended Rules") "if such transfer is based on consent" ((a) below). Furthermore, it is necessary to take the measures prescribed in the Amended Rules if "the third party in the foreign country has established a system for the protection of personal information" ((b) below).

(a) Information requiring provision "if such transfer is based on consent" (Article 11-3, paragraph 2 of the Amended Rules)

(i) Name of the foreign country

(ii) Information on such country's systems concerning the protection of personal information obtained in an appropriate and reasonable manner

(iii) Information on the measures for the protection of personal information taken by the third party in the foreign country

The issue with respect to (ii) above in particular, in connection with this obligation to provide information, is how companies are apprised of the systems for the protection of personal information in foreign countries.

(b) Necessary measures "if the third party in the foreign country has established a system for the protection of personal information" (Article 11-4, paragraph 1 of the Amended Rules)

(i) Periodically review, in an appropriate and reasonable manner, the status of personal data handling by the third party to whom personal data is transferred and whether there is a system in the foreign country where such third party is located that may affect its handling of personal data and the details of such system

(ii) Take necessary and appropriate measures in the event of a hindrance to the implementation of reasonable measures by the third party in the foreign country, and suspend the provision of personal data to the third party in the event of difficulty in ensuring the continued implementation of reasonable measures

One of the issues with the above measures is how to conduct a review of the personal data handling status of a company in a foreign country.

(c) Measures to be implemented

(i) Reconfirm whether personal data is actually being transferred outside of Japan: you will need to confirm whether your company transfers personal data outside of Japan and this recommendation applies even if you only do business in Japan.

(ii) Revise privacy policies: if personal data is being transferred outside of Japan on the basis of consent, you will need to consider revising your privacy policy to include the name of the foreign country to which you transfer personal data and an overview description of that country's system for protecting personal information.

(iii) Confirm details of contracts with foreign companies: if you have provided personal data to a company which "has established certain systems for the protection of personal information", it is necessary to continually review and confirm such company's personal data handling status.

(3) Common consultation matter: we often receive queries regarding the relevance of the country where a server is located, with respect to Article 24 of the Amendment Act. The Legislative Officer summarizes this point as follows.

First, if the operator of a server such as a cloud service does not handle the personal data saved on such server, it does not constitute provision of personal data to a third party in a foreign country (Article 24).

Where the server operator falls under the category of " third party in a foreign country", the relevant country that needs to be specified to the data subject is the country where the server operator is registered as a corporate body, rather than the country in which the server is located. If the country the server is located in is known, the data subject should be provided with information on the systems of that country to ensure accountability and transparency. Where there are servers in a multitude of jurisdictions, information on data protection systems of all relevant jurisdictions should be provided.

(4) Comments from our Frankfurt Office on the obligation to provide information regarding overseas transfer of personal data from a GDPR perspective

The GDPR also requires data controllers to provide data subjects with certain information regarding the transfer of their personal data outside the EEA. According to Article 13(1)(f) and 14(1)(f), GDPR, regardless of whether the transfer of data is justified by the data subjects' consent or other lawful basis, the data subjects must be informed of the following factors:

- "the existence or absence of an adequacy decision by the Commission" , i.e. whether the non-EEA recipient country is recognized by the EU Commission for having an adequate level of data protection. So far, there have been 12 countries, including Japan, which have been granted an Adequacy Decision by the EU Commission (full list of countries[2] with Adequacy Decisions); and
- if the non-EEA recipient country does not have an adequate level of data protection, what safeguards, under the GDPR, the data controller is using to protect the transferred personal data, such as among others, binding corporate rules or codes of conduct. The most commonly used safeguard at the moment is the standard contractual clauses approved by the EU Commission; and
- the means by which the data subjects can obtain a copy of the safeguards used or where they have been made available.

The above-mentioned information should be provided to data subjects when their data is collected. When the data is not collected directly from the data subjects, the information must be provided, at the latest, before the controller transfers the data.

4. Personally referable information

(1) Reasons for the establishment of the concept of personally referable information: internet browsing history of users, which does not constitute "personal information" , is collected and provided to third parties, as information that enables the individual to be identified. From a user's perspective, this makes it easier for them to access information that interests them. It has also become a vital component of certain business models that are now widespread.

In this regard, if a company identifies and uses a user's browsing history and the like without the user's knowledge, their rights and interests may be seriously infringed. To prevent this, the concept of "personally referable information" was introduced under the 2020 amendment, and new rules based on "third party provision of personal data" were established.

(2) What is personally referable information? "Personally referable information" is defined as "information relating to a living individual and which does not fall under personal information, pseudonymously processed information, or anonymously processed information" (main sentence of Article 26-2, paragraph 1 of the Amendment Act). Examples: internet browsing history and location information, which are not associated with an individual's name and cookies.

(3) Review of rules on personally referable information: Article 26-2, paragraph 1 of the Amendment Act provides for personally referable information as follows.

A personally referable information handling business operator... shall not, if it is assumed that a third party willacquire personally referable information (limited to personally referable information databases etc. (the same applies hereinafter)) as personal data, except in those cases set forth in each item of Article 23, paragraph (1), provide the personally referable information to a third party without confirming thosematters, pursuant to the rules of the Personal Information Protection Commission, set forth as follows.

(i) ...The principal' s consent...

(ii) [Omitted]

Under this provision, if a company provides another company with information that does not identify an individual, and it is anticipated that such company receiving the information will use the information in a way that makes it possible to identify an individual, it is necessary to obtain the data subject' s consent. In cases where it is anticipated that a third party acquires personally referable information as personal data, the data subject' s consent is required for this.

(4) Determining if it is anticipated that a third party acquires personally referable information as personal data

a. The receiving company has clearly indicated that it is acquiring personally referable information as personal data (no dispute): prior to the provision of personally referable information, the receiving company has clearly indicated to the providing company that it will collate the information to identify individuals.

b. The receiving company has not clearly indicated that it is acquiring personally referable information as personal data, and it is difficult to assess the situation: the Legislative Officer has specified that it should be determined

---

[2] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

whether it can be reasonably anticipated, in light of objective circumstances such as the status of transactions, that such third party will acquire personally referable information as personal data that could be generally recognizable. An example is where a receiving company will link personally referable information that it has received with other information such as names.

c. The contract between the providing company of personally referable information and the receiving company stipulates that receiving company will not acquire personally referable information as personal data: in this scenario, the providing company would not normally anticipate that such third party would acquire the personally referable information as personal data. Therefore, Article 26-2, paragraph 1 of the Amendment Act would likely not apply.

However, the Legislative Officer has stated that where the receiving company is a large-scale internet mail order business operator, Article 26-2, paragraph 1, may apply if such business operator holds customer information of an unspecified number of people, and if there is a high probability that the information will be collated with other customer information and used as personal data. This principle would apply regardless of what is stated in the relevant contract

(5) Other issues for consideration in addition to the above:

(i) Method of obtaining consent

(ii) Record of confirmation that consent has been obtained

(iii) Measures if personally referable information is transferred overseas

(iv) Measures if the handling of personally referable information is outsourced

(6) Comments from our Frankfurt Office on personally referable information from a GDPR perspective

1. Definition of personal data under the GDPR

Under Article 4(1) of the GDPR, "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" . The GDPR does not have a separate definition for "personal-related information" like the Japanese data protection law. Even though one data item, alone, may not identify a natural person, it is possible that such data can identify an individual after it is combined with other data, and thus can constitute personal data. In other words, data such as Internet browsing history, location information and cookies, which are considered "personal-related information" under Japanese data protection law, are also defined as "personal data" under the GDPR and are protected in the same manner as any other personal data categories such as name, ID number or email address.

Data is not considered as "personal data" under the GDPR only when it is made irreversibly anonymous, and the data subject can no longer be identified by any means. Anonymized data is therefore not protected by the GDPR. Data that has been encrypted or pseudonymized is still considered "personal data" as it can potentially be used to re-identify a person, when being decoded or combined with other data.

2. Controllers' obligations towards personal data

Provided the data is considered "personal data", it is protected under the GDPR and data controllers and processors have to fulfil their obligations towards such data. Each data controller and processor shall be independently responsible for complying with its obligations under the GDPR, unless:

(i) as joint controllers, they have an agreement among themselves regarding who shall be responsible for certain obligations, including the obligations to obtain data subjects' consent when required (Article 26(1) GDPR); or

(ii) in a controller/processor relationship, in which the processor shall only process personal data under the controller's instruction, it is the controller's sole obligation to make sure data subjects have given valid consent, if required.

However, Article 11 of the GDPR provides an exemption that "if the purposes for which a controller processes personal data do not or no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation" .

Even if the processor can potentially use the personal data from the controller to identify the data subjects, it may not be permitted, under the controller' s instruction, to do so. If, regardless of the foregoing, the processor attempts to identify the data subjects for its own purposes, the processor will be considered an independent controller in respect of that personal data and must then be independently responsible for, among other things, ensuring a lawful basis for its processing activities, e.g., obtaining consent (Article 28(10) GDPR).

When an independent controller A shares personal data that it cannot use to identify the data subjects, to another independent controller B who might be able to use such data to identify the data subjects, the GDPR does not require controller A to ensure that controller B has obtained the data subjects' consent. In respect of controller B' s independent processing activities after receiving the data from controller A, it is controller B' s sole obligation to inform the data subjects of how it processes their data and to request their consent (if consent is required). If controller B fails to comply with this obligation, it will be solely liable to the data subjects.

However, if controller B is not located in an EEA country or a country with an Adequacy Decision system (Article 45 GDPR), controller A must ensure that controller B will comply with the GDPR basic principles by applying one of the appropriate safeguards under Article 46(2) GDPR. The Standard contractual clauses by the EU Commission, as the most commonly used safeguard, requires the data exporter (i.e. controller A) to use reasonable efforts to determine that the data importer (i.e. controller B) is able to satisfy its legal obligations under the clauses. In this case, controller A might be held liable to data subjects if it shares personal data with controller B when it is aware of the fact that controller B is actually unable to ensure compliance with GDPR principles (e.g. it is unable to obtain data subjects' consent where required). The rule for international transfer of data is a unique GDPR rule requiring a data sender to exercise some control over its data recipient, which is to an extent similar to the "personal-related information" rules in the Japanese data protection act.

In short, GDPR does not distinguish personal data and personal-related information and there are thus no special rules for personal-related information under this Regulation. Data controllers and processors shall be independently responsible for complying with their obligations under the GDPR or under equivalent applicable law, unless in the case of joint controllership or when the data importer is not located in an EEA country or a country with an Adequacy Decision system.

5. Obligations in the Event of a Personal Data Breach

(1) Reasons for the establishment of obligations in the event of a data breach: prior to the 2020 amendment, legal liability did not arise in the event of a personal data breach. Instead, it was merely stipulated by "public notice" that a report be made to the PPC and many companies have made such personal data breach reports in response to the public notice, but the making of such a report was not mandatory.

(2) Obligations in the event of a data breach: Article 22-2, paragraph 1 of the Amendment Act provides for reporting obligations to the PPC in the event of a data breach as follows.

A personal information handling business operator shall, pursuant to the rules of the Personal Information Protection Commission, report to the Personal Information Protection Commission when there is a leakage, loss or damage or other situation concerning the security of its handled personal data. This, however, shall not apply in cases where the personal information handling business operator, who has been entrusted by another personal information handling business operator to conduct a whole or part of the said handling of personal data, has already informed of such occurrence to the entrusting personal information handling business operator, in accordance with the rules of the Personal Information Protection Commission.

Furthermore, the main clause of Article 22-2, paragraph 2 of the Amendment Act provides for reporting obligations to the data subject in the event of a data breach as follows.

> In those cases prescribed by the preceding paragraph, a personal information handling business operator…shall, pursuant to rules of the Personal Information Protection Commission, notify a principal of the occurrence of a data breach. This, however, shall not apply when it is difficult to inform a principal and when necessary alternative action is taken to protect a principal's rights and interests.

(3) Obligation to report to the PPC: in practice it is important to determine "what sort of data breach" gives rise to an obligation to report to the PPC (see (a) below) and "by when" such report must be made (see (b) below)

a. "What sort of data breach" gives rise to an obligation to report? Article 6-2 of the Amendment Rules stipulates the following cases.

> (i) If the breached personal information includes sensitive information
>
> (ii) If property damage is likely to occur as a result of wrongful use of the breached personal information
>
> (iii) If the data breach is likely to have occurred for a wrongful purpose (intentionally due to unauthorized access, etc.)
>
> (iv) If the number of concerned data subjects pertaining to the breached personal data exceeds 1,000

b. "By when" does the data breach have to be reported? Article 6-3 of the Amendment Rules provides for:

> Step 1:
> Preliminary report → promptly after becoming aware of any of the situations listed in (i) through (iv) above
>
> Step 2:
> Confirmed report → within 30 days after becoming aware of the data breach situation (within 60 days in the case of (iii) above)

(4) Addressing legal obligations in the event of a data breach

a. Develop specific internal procedures from the occurrence of a data breach to reporting to the PPC, as follows

> (i) Incident report
>
> (ii) Department responsible for responding to data breaches
>
> (iii) Simple flow chart outlining process for responding to data breaches

The above internal procedures are important in ensuring that timely reports are made within the periods specified under the APPI.

b. Employee training: if an employee of any given company department or division is not aware of the reporting deadline stated above, and the report to the PPC is delayed, this will likely constitute a violation of the APPI by the company.

Therefore, it is necessary to provide extensive training to employees working in various departments of the company and to make them aware of the measures to be taken in the case of a data breach, as mentioned above.

c. Contracts with subcontractors, etc.: if personal data is transferred to a subcontractor, it is necessary to address any data breach that occurs at the subcontractor. You should review the contract with the subcontractor so that you are able to promptly obtain a report of the data breach from the subcontractor and take measures, such as investigating the cause of the data breach.

d. If you retain personal data of foreign residents you should report to the relevant foreign authorities and notify the data subject in accordance with the laws of the relevant foreign country.

(5) Comments from our Frankfurt Office on obligations in the event of a data breach from a GDPR perspective

Article 33(1) of the GDPR sets out a general notification requirement in case of a data breach. In particular, a controller shall without, undue delay and, where feasible, no later than 72 hours after having become aware of a data breach, notify the breach to the competent supervisory authority, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, the controller must provide reasons for the delay.

For the exemption under Article 33(1) GDPR that is only applicable where there is no risk to natural persons, it is vitally important that the controller should not only seek to contain the data incident, but it should also assess the risk that could result from the breach, immediately upon becoming aware of it.

There is no precise definition of when a data breach results in a risk to the rights and freedoms of data subjects. In its guidelines, the EDPB suggests several factors for controllers to consider when assessing the risks associated with a data breach:

- the type of breach (e.g., data leakage or data lost);
- the nature, sensitivity, and volume of personal data;
- the ease of identification of individuals;
- the severity of consequences for individuals;
- the special characteristics of the individual and the data controller.

Recital 75 of the GDPR gives some examples of the risks to rights and freedoms and suggests that risks should be broadly interpreted to include physical and material damage, as well as non-material damage such as discrimination, identity theft, fraud, financial loss, reputation damage or unauthorized reversal of pseudonymization, etc. In practice, data controllers are likely to notify data breaches in most cases, rather than take the risk of not notifying such breaches and then later being found to have committed a violation.

In the event that the breach poses a high risk to natural persons (e.g. when sensitive data is involved), the controller will have to notify not only the supervisory authority, but also the affected data subjects (Article 34(1) GDPR).

On the other hand, the EDPB's guideline states that if, for example, the breached data is publicly available or properly encrypted to be unintelligible to unauthorized parties, it is considered a "no-risk" situation and the controller will be exempted from the notification obligation.

Regarding the data breach notification procedure, it is not compulsory but it can be recommended as best practice for data controllers and processors to conduct trainings and have internal policies in place for their employees regarding action that needs to be taken in the case of a data breach.

In addition, Article 33(5) of the GDPR also requires controllers to keep reports of all data breaches (not only the breaches that pose risks on natural persons), including the facts relating to the breach, its effects, and the remedies taken. The competent supervisory authority may ask for such data breach reports at any time, in order to review and confirm the controllers' accountability.

Fines for non-compliance with the data breach notification and documentation obligation under Article 33 of the GDPR can be up to 10 million Euro or up to 2% of the controller's worldwide turnover of the preceding year, whichever is higher (Article 83(4)(a) GDPR).

6. Pseudonymously Processed Information

(1) Reasons for the establishment of rules on "pseudonymously processed information"

Under the 2015 amendment, the concept of "anonymously processed information" was established to create an environment conducive to the proper utilization of big data. Anonymously processed information is processed so that a specific individual cannot be identified and the original personal information cannot be restored. Anonymously processed information can be used for purposes other than the intended purpose or provided to a third party without the data subject's consent.

However, there were also cases in which, as a part of security control actions, information was processed to a degree not equivalent to the creation of anonymously processed information (such as the deletion of names), so that a specific individual could not be identified from the processed data alone (pseudonymization). "Pseudonymized" personal information is anticipated to be utilized to ensure a certain level of security through relatively simple processing while also maintaining its utility as data.

(2) What is "pseudonymously processed information" ?

"Pseudonymously processed information" is information relating to an individual that can be generated from personal information, so that a specific individual cannot be identified unless it is collated with other information. It also has the following characteristics.

(i) Restricted to internal use for analysis by the operator

(ii) Eased obligations and less restrictions in responding to requests from data subjects

(iii) Eased reporting obligations in the event of a data breach

(3) Areas where "pseudonymously processed information" is anticipated to be used: according to the Legislative Officer, it is anticipated that "pseudonymously processed information" will be used in cases such as the following.

(i) Cases where internal analysis is conducted for purposes that do not correspond to the initial purpose of use or for new purposes for which it is difficult to determine whether they correspond to the initial purpose of use (e.g., cases in which the information is used in research data sets in the medical and pharmaceutical fields, where unique values in a data set are significant, or cases where the information is used in data sets for machine learning models, such as for fraud detection)

(ii) Cases where personal information for which the purpose of use has been achieved is processed as pseudonymously processed information and stored because it may be used for statistical analysis in the future

(4) Comments from our Frankfurt Office on pseudonymously processed information from a GDPR perspective

Article 4(5) GDPR defines "pseudonymization" as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". A common method of pseudonymization is to replace one attribute such as name, social security number, date of birth etc. in a dataset by e.g., a randomly assigned code. After this process, as pseudonymized data can still be used to indirectly identify the data subject, it is still considered to be personal data protected under the GDPR. The additional information which can be used to re-identify data subjects must be kept separately from the data it relates to by means of technical or organizational measures.

Under the GDPR, pseudonymization is not only encouraged as a means of data security (Article 32(1)(a) GDPR). The technique is also linked to the more generalized duty of "data protection by design" (Article 25(1) GDPR) and to data minimization safeguards connected to processing for archiving purposes, scientific or historical research purposes or statistical purposes (Article 89(1) GDPR).

Pseudonymization is not made a compulsory duty, but rather a recommended technique according to the GDPR wordings. However, some EU Member States' laws still impose strict pseudonymization requirements. For example, Article 71(1) of the German Protection Act stipulates that "personal data shall be rendered anonymous or pseudonymized as early as possible and as far as possible, in accordance with the purpose of processing". It is nevertheless controversial whether the EU Member States are permitted, under the GDPR, to make pseudonymization a compulsory measure for data security in its national rules.

7. Future Issues in This Series

In subsequent editions, we will cover topics such as "international transfers of data collected through video", "the use of location information for business purposes", "the medical, pharmaceutical and healthcare fields", "the financial sector", "internal controls and data", "Chinese law", "Korean law", "Vietnamese law", and "Taiwanese law".

Fumiaki Matsuoka
Attorney (Bengoshi), Japan
Partner
E: fumiaki.matsuoka@aplaw.jp
> View Profile

Haruhi Kumazawa *
Advisor
* No qualification as a lawyer (Does not provide legal advice)
> View Profile

Akiko Hiraoka
Attorney (Bengoshi), Japan
Associate
E: akiko.hiraoka@aplaw.jp
> View Profile

Ciaran Rose
Attorney (Bengoshi), Japan
Associate
E: ciaran.rose@aplaw.jp
> View Profile

Satoshi Fukuhara
Attorney (Bengoshi), Japan
Associate
E: satoshi.fukuhara@aplaw.jp
> View Profile

Shohei Shidara
Attorney (Bengoshi), Japan
Associate
E: shohei.shidara@aplaw.jp
> View Profile

Frank Becker
Admitted in the Federal Republic of Germany*
(Atsumi Sakai Jannsen Rechtsanwalts- und Steuerberatungsgesellschaft mbH**)
E: frank.becker@aplaw.de
> View Profile

* Not Registered as a Foreign Lawyer and not practicing law in Japan
** A legal and tax advisory professional corporation registered in Germany

Please contact our PR staff to subscribe our newsletter.
E: prcorestaff@aplaw.jp

Atsumi & Sakai
Tokyo Office: Fukoku Seimei Bldg. (16F), 2-2-2 Uchisaiwaicho, Chiyoda-ku, Tokyo 100-0011, Japan
London Office: 4th Floor, 50 Mark Lane, London, EC3R 7QR, United Kingdom
Frankfurt Office: OpernTurm (13 F), Bockenheimer Landstraße 2–4, 60306 Frankfurt am Main, Germany
General enquiries: info@aplaw.jp
Website: www.aplaw.jp/en