ANDERSON MŌRI & TOMOTSUNE

AMT NEWSLETTER

December 2020

2020 Amendment of the Act on the Protection of Personal Information

Nobuhito Sawasaki / Ryo Murakami

The bill to amend the Act on the Protection of Personal Information was passed by the Diet on June 5, 2020. This amendment is a follow-up on the Japanese government's policy to review the legal system every three years, as stipulated by the 2015 amendment to the Act which came into full force on May 30, 2017. The 2020 amendment makes reforms to the Act to strengthen the protection of the rights of principals who may be identified by personal information, as well as the supervisory and enforcement powers of the Personal Information Protection Commission of Japan. The amendment also aims to promote the utilization of data in society. The effective date of the amendment will be decided in the future, which will be no later than two years from June 12, 2020 (the date of promulgation of the amendment). This Newsletter explains the contents of the amendment and what compliance preparations business operators should make by the effective date.

1. Overview of the 2020 Amendment of the Act on the Protection of Personal Information

On June 5, 2020, at the 201st ordinary session of the Diet, the bill for the Partial Amendment of the Act on the Protection of Personal Information (the "Act on the Protection of Personal Information" is hereinafter referred to as the "Act[1]") was approved. This amendment (the "Amendment"; and the Act so amended is hereinafter referred to as the "Amended Act") was promulgated on June 12, 2020. The Amendment, except for certain provisions, will take effect on a date to be stipulated by a cabinet order, which will be no later than two years after the promulgation of the Amendment. The Amendment is a follow-up on the Japanese government's policy to "review the situation after the enforcement of the new Act (*Editor's Note: this refers to the 2015 amendment of the Act*) by taking into account international trends concerning the protection of personal information, development of information communication

[1] Translations of the current Act and related regulations and materials are available at https://www.ppc.go.jp/en/legal/.

technology and the creation and development of new industries resulting from such technologies that utilize personal information, and to make necessary reforms every three years based on the results of such review," as stipulated in Article 12(3) of the Supplementary Provisions of the 2015 amendment of the Act (which came into full force on May 30, 2017; the "2015 Amendment").

The contents of the Amendment are as follows.

(1) Reinforces the general obligations of personal information handling business operators[2] to properly handle personal information[3]

- Expressly stipulates the prohibitions on improper use of personal information; and
- Creates an obligation to report certain personal data leakages to the Personal Information Protection Commission (the "PPC") and notify the affected principals of the same.

(2) Reinforce the principal's rights concerning retained personal data[4]

- Grants a principal the right to designate the method of disclosing retained personal data;
- Creates a right to demand for the suspension of use of personal data when a leak has occurred or "there is a possibility for the principal's rights or just interests to be infringed";
- Amends the definition of retained personal data; and
- Adds certain new items to the list of information that business operators must disclose concerning retained personal data.

(3) Reinforces the protection of principals' interests concerning third party provision of personal data[5]

- Adds certain new items to the list of information that business operators must notify to the PPC upon the provision of personal data to third parties using the "opt-out" method (the "opt-out" method refers to a business operator's provision of a principal's personal data to a third party upon notification of certain information to the PPC and disclosure of the same, without obtaining the consent of the principal, and on the condition that the business operator will cease such provision upon a request by the principal);
- Prohibits business operators from (i) providing improperly acquired personal data to third parties using the opt-out method, or (ii) providing personal data that has already been provided

---

[2] Business operators that use personal information databases etc. for their businesses (Article 2(5) of the Act, Article 2(5) of the Amended Act).

[3] Information concerning a living individual which, alone or by being readily collated with other information, identifies a specific individual, or information that includes an individual identification code such as an Individual Number (a 12-digit ID number issued to all citizens and residents of Japan), passport number, resident register code, or DNA information (Article 2(1) of the Act, Article 2(1) of the Amended Act).

[4] Personal data which a personal information handling business operator has the authority to disclose, correct, add, delete, suspend use of, erase, and cease providing to third parties (Article 2(7) of the Amended Act).

[5] Personal information that comprises a database, etc. ("personal information database etc.") that is systematically structured to enable a person to easily search for particular personal information (Article 2(6) of the Act, Article 2(6) of the Amended Act).

by the opt-out method to third parties via the opt-out method again;

- Creates an obligation for business operators to provide certain information on foreign systems for personal information protection to the principal when providing personal data to a third party located in a foreign country;
- Creates an obligation for business operators to confirm and record certain matters when providing information that is expected to become personal data only when received by the recipient;
- Creates the principal's right to demand for disclosure of records concerning the provision of personal date to third parties; and
- Adds certain items to the list of information that business operators must disclose upon joint use ("joint use" means sharing and jointly using personal data with third parties upon disclosure or notification to the principal, without obtaining the consent of the principal).

(4) Introduces a new concept of "pseudonymously processed information" and adds related provisions

Adds a new definition of "pseudonymously processed information," which means information which is processed in a way that prevents an individual from being identified unless the information is collated with other information. In connection with this, the Amendment also stipulates the obligations of business operators that handle such information, and exempts them from the obligation to respond to requests for disclosure or suspension of use, etc. by the principal even if such information falls under the definition of personal data.

(5) Expands the scope of extraterritorial application

To date, the provisions in the Act subject to extraterritorial application were limited only to certain provisions. The Amendment expands the scope of the extraterritorial application to all the provisions in the Amended Act. The situations and business operators that are subject to the extraterritorial application will also be expanded to broadly cover situations where business operators handle information relating to an individual in connection with the provision of goods or services to persons located in Japan.

(6) Strengthens the PPC's enforcement power and criminal penalties

Authorizes the PPC to disclose the name of business operators that have breached an order made by the PPC. Furthermore, the maximum fine that may be imposed on a legal entity for a breach of a PPC order or the provision or theft of a personal information database etc. for the purpose of gaining an illicit profit will be raised to JPY 100 million. The maximum limit for some other criminal punishments will also be raised.

(7) Others

Amends certain provisions concerning accredited personal information protection organizations, and introduces provisions concerning service by the PPC of demands for reports, recommendations, or orders.

2. Details of the Amendment and Expected Effects on Handling of Personal Information

(1) Reinforcement of the general obligations of personal information handling business operators to properly handle personal information

Prohibition on improper use

The Amendment creates a new provision stipulating the general obligation of personal information handling business operators not to "use personal information in a manner that encourages or is likely to encourage illegal or improper conduct" (Article 16-2 of the Amended Act).

With respect to this new provision, a report published by the PPC named "'The Every-Three-Year Review' of the Act on the Protection of Personal Information – Outline of the System Reform" (December 13, 2019; the "System Reform Outline"[6]) explains that the PPC has recognized that there are some cases where personal information is being used in a manner that cannot be said to be "proper" even though such cases are not illegal under the current Act, and that such cases of improper usage shall also be expressly prohibited. This means that cases where the use of personal information is not "proper" that could result in the infringement of an individual's rights and interests, including conduct that currently does not constitute a clear breach of any provisions of the Act, will be prohibited under the Amended Act. Business operators will therefore be required to take further measures to assure that their officers and employees use personal information in a socially "proper" manner.

A newly created obligation to report and notify certain personal data leakages

The Amended Act stipulates an obligation to make a report to the PPC and to the affected principals in the event of a leak, loss or damage of personal data that meets certain criteria stipulated by the PPC's Enforcement Rules for the Act on the Protection of Personal Information (the "Enforcement Rules") to be amended by the PPC by the effective date of the Amendment (Article 22-2 of the Amended Act).

The current Act does not contain any express provisions on the reporting of incidents where personal data is leaked, lost or damaged. The only relevant regulations are in the PPC's guidelines ("Guidelines on actions to be taken if a personal data leakage, etc. occurs"), which state that business operators should "make efforts to report" promptly to the PPC, and that "it is advisable" to contact the principals regarding the circumstances of the leakage, etc. or enable the principals to readily comprehend the situation (by contrast, the guidelines concerning the protection of personal information for the financial industry sets out more specific details on the measures that should be taken, such as stating that personal data leakages, etc. "shall be immediately reported to the supervising authorities"

---

[6] A tentative translation of the System Reform Outline is available at https://www.ppc.go.jp/en/aboutus/roles/international/cooperation/20200124/.

and “the underlying facts and other information shall be promptly notified to the principal.”).

Under the Amended Act, it will become mandatory to report on the details concerning certain incidents where personal data is leaked, lost or damaged, and a breach of this obligation will be subject to enforcement actions by the PPC, such as the issuance of recommendations or orders. The criteria for incidents to be reported and the method of making a report have yet to be decided by the relevant provisions in the PPC’s Enforcement Rules and guidelines (to be amended by the PPC by the effective date of the Amendment). At present, based on the System Reform Outline, it is expected that the leak of a certain number of pieces of personal data or leak of “special care-required personal information”[7] will become subject to those obligations, and that business operators would be required to make immediate announcements on certain matters first, and then follow up by making a detailed report including an analysis of the causes of the incident and corrective measures to prevent the recurrence of such incidents.

Preparation by the effective date

We believe many business operators have set out in their internal regulations a process to grasp the facts, make a report and contact the affected principals in the event that personal information is leaked, lost or damaged, and that such process reflects the requirements of the current Act and the guidelines currently in effect. Such business operators would need to revise their internal regulations to reflect the contents of the Amendment and the Enforcement Rules.

(2) Reinforcement of the principal’s rights concerning retained personal data

Grant to a principal of the right to designate the method of disclosing retained personal data

The current Act grants the principal the right to demand disclosure of retained personal data identifying such principal, and with respect to this right, the Act stipulates that disclosure shall be made in writing in principle, or alternatively by another method that was agreed with the principal, if any (Article 28(2) of the Act and Article 9 of the Cabinet Order for the Enforcement of the Act (the “Cabinet Order”)). The Amended Act, from the perspective of promoting digitalization of disclosure (as explained in the System Reform Outline), allows the principal to choose a method of disclosure from those stipulated in the Enforcement Rules which are to be established by the PPC at a future date (i.e. granting the principal the right to designate the disclosure method in advance), and mandates disclosure in writing if disclosure by the method designated by the principal is difficult for cost-related or other reasons (Articles 28(1)-(2) of the Amended Act).

Creation of a right to demand for suspension of use where the principal’s rights or just interests will be or may likely be infringed

[7] “Special care-required personal information” is defined as information that is designated by the Cabinet Order for the Enforcement of the Act as delicate information such as medical histories, arrest records and criminal records (Article 2(3) of the Act, Article 2(3) of the Amended Act).

Next, the Amendment expanded the grounds for demanding the suspension of use or erasure of retained personal data. The current Act limits the grounds for such demands to situations (i) where the retained personal data was being used for purposes other than the purposes specified in advance, or (ii) where the relevant retained personal data was not properly acquired. The Amendment adds the following situations to this list: (iii) where there is a breach of the newly created provision prohibiting the improper use of personal information (Article 16-2 of the Amended Act), (iv) where there is no longer a need to use the retained personal data, (v) where personal data is leaked, lost or damaged, and (vi) "other cases where the handling of retained personal data that identifies the principal would possibly infringe that principal's rights or just interests" (Articles 29(1), (5) of the Amended Act). Under the Amended Act, business operators must make a legal decision as to whether the use of retained personal data "would possibly infringe that principal's rights or just interests", which is an abstract requirement, although the PPC may publish some examples of cases that meet that requirement in its guidelines.

Preparation by the effective date

Business operators would need to revise their internal regulations and guidelines to reflect the contents of the Amendment. Business operators that have mainly disclosed demanded personal data in writing in accordance with the current Act would need to stipulate a new process to deal with the relevant disclosure method designated by the principal. With respect to (iv) above, although the current Act already imposes a duty to make best efforts to erase unnecessary personal data without delay (Article 19 of the Act), which remains unchanged in the Amended Act (Article 19 of the Amended Act), it is strongly recommended that after the effective date of the Amendment, business operators should erase retained personal data if it becomes no longer necessary to retain the same, so that unnecessarily retained personal data will not be subject to any demands for disclosure.

Other incidental amendments

The Amendment also revises the definition of "retained personal data." Under the current Act, personal data that is to be deleted within six months from the date of its acquisition is excluded from the scope of this definition (Article 2(7) of the Act, Article 5 of the Cabinet Order). However, the Amendment has deleted this exclusion (Article 2(7) of the Amended Act). Therefore, after the effective date, business operators should be careful not to inadvertently refuse a demand made by a principal with respect to information that is to be erased within a short period which is currently not subject to disclosure.

The Act provides that business operators must make certain types of information on retained personal data readily accessible by the principals (such as the purposes of use of the personal information). The Amendment adds the following to the list of such information: (i) the address of the business operator, and (ii) the name of the business operator's representative (if the business operator is a legal entity) (Article 27(1) of the Amended Act). It is also expected, based on the contents of the System Reform Outline, that some other additional types of information will be added to the list via amendment of the Cabinet Order.

(3) Reinforcement of the protection of principals' interests concerning third party provision of personal data

The Amendment makes various reforms to reinforce the protection of principals' interests concerning the provision of personal data to a third party.

Amendment concerning opt-out (1)

With regard to the provision of personal data to third parties using the "opt-out" method, the 2015 Amendment stipulated an obligation for business operators to notify the PPC of certain matters in advance (such as the type of personal data to be provided and the method of provision to third parties), and to notify principals of the same or make such information readily accessible by the principals (Article 23(2) of the Act). Under the Amended Act, the following will be added to the list of matters subject to this notification and disclosure obligation: (i) the name, address and name of the representative of the personal information handling business operator that is providing personal data, (ii) the method of acquiring the personal data that is to be provided, and (iii) other matters stipulated by the PPC's Enforcement Rules (Article 23(2) of the Amended Act). The purpose of these additions is to strengthen the PPC's enforcement power by allowing it to collect the necessary contact information.

Business operators that are providing personal data to third parties by the opt-out method must revise the contents of their notices to the principals or the notices on their websites to reflect the above amendment.

Amendment concerning opt-out (2)

The current Act provides that business operators cannot provide special care-required personal information by the opt-out method. Under the Amended Act, in addition to special care-required personal information, business operators must not provide the following to third parties via the opt-out method: (i) personal data that was acquired in breach of the provision mandating proper acquisition (Article 17(1) of the Amended Act), or (ii) personal data that was received through the opt-out method (Article 23(2) of the Amended Act). The aforesaid item (ii) means that any personal data that was provided to a business operator through the opt-out method cannot be further provided to a third party through the opt-out method. The purpose is to prevent the transfer and distribution of personal data without the involvement of the principal.

A newly created obligation to provide information on the systems in foreign countries

The 2015 Amendment created special requirements for business operators that provide personal data to a third party located in a foreign country. In summary, the 2015 Amendment imposed an obligation on business operators to obtain the principal's consent in advance when they provided personal data to a third party located in a foreign country, but exempted them from such obligation where

they provided personal data to service contractors or other entities (typically group companies) that jointly used the same personal data, on the condition that the party receiving the personal data was obligated to take protective measures equivalent to those required in the Act.

In addition to the above requirements, the Amendment (i) requires business operators that purport to provide personal data to a foreign third party upon the principal's consent to provide information on the system for protection of personal information in such foreign country, as well as information on protective measures to be taken by such third party to the principal in advance, and (ii) requires business operators that have provided personal data to a foreign third party without the principal's consent (as permitted in the Act) to take necessary measures to ensure that such third party will continuously implement protective measures for the provided personal data and to provide the principal with the relevant information upon request (Articles 24(2)-(3) of the Amended Act). The details on these matters will be stipulated in the PPC's Enforcement Rules.

We believe that many business operators may be providing personal data to their service contractors or group companies in foreign countries without the principal's consent, after having executed a service agreement or established group information management regulations obligating the recipient of the personal data to take protective measures equivalent to those required in the Act (as permitted under the Act). The new obligation explained in (ii) above will apply to this situation, and therefore business operators would need to review their provisions concerning audits on the group's information management regulations and service contracts in order to establish a procedural flow to provide information if requested from the principal, and to make other necessary adjustments in their regulations, contracts and practices in preparation for the effective date of the Amended Act and the new Enforcement Rules.

Obligations concerning provision of information which is expected to constitute personal data when received by the recipient

Next, the Amendment creates new obligations for business operators providing information that is not personal data for the providing party but which is expected to constitute personal data when received by the recipient. The Amendment requires the providing party in this case (i) to confirm that the principal has given consent to the acquisition by the recipient of such information (and if the receiving party is located in a foreign country, that the principal has been provided with information on the system for protecting personal information in such foreign country and protective measures to be taken by the receiving party), and (ii) to maintain records on this confirmation (Article 26-2 of the Amended Act). On this basis, the acquisition of such consent from the principal is also obligated in the Amended Act.

As mentioned in the System Reform Outline, examples of such information that may be expected to become personal data when received by the recipient would be identifier information such as cookies, and information exchanged on DMPs (Data Management Platforms, which means platforms for the collection and analysis of user data on the internet) that contains identifier information. However, the information subject to these new obligations would not be limited to the foregoing; rather, the obligations

will generally apply to the provision of “personally referable information” that constitutes a “personally referable information database, etc.” by a “personally referable information handling business operator” in a situation where the information is expected to constitute “personal data” when received by the recipient, because the recipient could easily collate the information with other information (such as the name of the principal) to identify the principal. “Personally referable information” means any information concerning a living individual which does not fall under “personal information,” “anonymously processed information” or “pseudonymously processed information.” “Personally referable information database, etc.” means a database structured to easily search personally referable information. “Personally referable information handling business operator” means a business operator that uses a personally referable information database, etc. for its business (Article 26-2 (1) of the Amended Act).

While the current Act obligates business operators that provide personal data to a third party to keep records of such provision (subject to certain exceptions), it is not clear whether the providing party would be obligated to keep records of any third party provision of information that would become personal data only when received by the recipient (Article 25 of the Act). Even the PPC’s guidelines do not expressly make any mention of this issue. However, the Amendment expressly stipulates, and thus makes it clear, that the principal’s consent must be obtained for such provision, and that the providing party has the obligation to confirm that such consent is obtained. Furthermore, with respect to the provision of ordinary personal data (not “personally referable information”), provision incidental to business succession, consignment (i.e. provision to service contractors), or joint use is not deemed to be provision to a “third party” for the purposes of these regulations, and the principal’s consent is unnecessary (Article 23(5) of the Act, Article 23(5) of the Amended Act). By contrast, the above-mentioned new obligations regarding the provision of personally referable information extends to business succession, consignment and joint use.

The principal’s right to demand for disclosure of records concerning third party provision

The current Act requires business operators that provide personal data to third parties to keep records of such provision, and those that receive personal data from third parties are obligated to confirm certain facts (such as the identity of the providing party and how it has acquired the provided information) and to keep records of such confirmation. The Amendment requires business operators to disclose those records upon a request by the principal (Article 28(5) of the Amended Act).

These obligations to keep records are applicable only where third party provision is based on the principal’s consent or the opt-out method, and the provision of personal data in respect of consignment and joint use are excluded from such recording obligations (which in practice are commonly used exceptions to the recording obligations). Therefore, we believe that in actual practice, there may not be many occasions for such records to be created. However, business operators that have created such records pursuant to the Act must ensure that they create records in such a manner that the records can be disclosed to the principal, and establish a procedural flow to respond to any demand for disclosure from the principal.

Disclosure upon joint use

With respect to the joint use of personal data, the current Act allows it on the condition that the business operator notifies the principal of, or makes readily accessible by the principal, the following information: (i) the fact that the personal data is subject to joint use, (ii) the items of personal data to be jointly used, (iii) the identities of the joint users, (iv) the purpose of use by the joint users, and (v) the name of the party that is responsible for managing the personal data (Article 23(5)(iii) of the Act). There is no change to this mechanism itself, but the Amendment adds the following to the matters that must be notified: (vi) the address of the party that is responsible for managing the personal data, and (vii) the name of the representative of such party if it is a legal entity (Article 23(5) of the Amended Act).

Under the current Act, a business operator who wishes to make any changes to the notified information in (iv) or (v) above may do so by amending the existing notice that had been issued to the principals previously and giving them advance notice of such amendment. However, it is commonly understood that any changes to (i) to (iii) above cannot be made using the aforementioned method. As such, in the event of any changes to (i) to (iii) above, joint use can be commenced only after the business operator has issued a new and separate notice to the principals regarding such changes. The Amendment has revised this mechanism slightly, so that advance notice is required when making changes to the responsible party, and post-facto notice must be given without delay for a change in the name of the responsible party (e.g. a case where the responsible party remains the same but has changed its corporate name), the address of the party and the name of its representative (Article 23(6) of the Amended Act).

As far as we know, when business operators conduct business or marketing jointly with their business partners, they quite often share and jointly use personal data by publicizing the above-mentioned information in their privacy policies or other similar notices. Although this may only be a matter of formality, business operators would be required to update their privacy policies, etc. in response to the addition of the above-mentioned items that must be disclosed.

(4) Introduction of a new concept of “pseudonymously processed information”

What it means

The Amendment introduced the definition of “pseudonymously processed information” (Article 2(9) of the Amended Act) and created new provisions relating to this new concept (Article 2(10), Article 35-2, and Article 35-3 of the Amended Act). The purpose of this new mechanism is to exempt business operators from certain obligations regarding the handling of personal data and promote utilization of such information in anticipation that it would mainly be used for internal analyses by companies, in exchange for imposing new obligations for the proper handling of this type of information. In particular, even if pseudonymously processed information falls under the definitions of personal information or personal data (which means it would otherwise be subject to the existing regulations on personal information and personal data), the Amendment expressly excludes the application of the provisions on

(i) the restriction on the extent to which business operators can change the purposes of use of personal information (Article 15(2) of the Amended Act), (ii) the reporting of leakages (Article 22-2 of the Amended Act), and (iii) the demand for disclosure, erasure, deletion, correction, etc. (Article 27 to Article 34 of the Amended Act). Based on a similar idea, the 2015 Amendment had already introduced a series of provisions concerning "anonymously processed information." While anonymously processed information must be processed to such an extent that the principal can no longer be identified, pseudonymously processed information means information that is processed to such an extent that the principal can only be identified by collating it with other information, which could be created more easily than anonymously processed information. Indeed, some companies may have already taken measures to manage the personal information retained by them by masking or deleting identifier information as part of their security control measures. On this assumption, and as mentioned in the System Reform Outline, the Act purports to promote the utilization of such information from the perspective of improving the international competitive power of Japanese companies.

Definition of "pseudonymously processed information"

"Pseudonymously processed information" is defined as information obtained by processing personal information so that a specific individual cannot be identified unless the information is collated with other information, where (i) for personal information that contains individual identification codes, these codes shall be deleted entirely or be replaced with other descriptions using a method with no regularity that can enable the individual identification codes to be decoded, and (ii) for other personal information, part of such information (such as the name of the principal, etc.) shall be deleted or replaced with other descriptions using a method with no regularity that can enable such information to be decoded (Article 2(9) of the Amended Act). This definition may appear similar to the definition of "anonymously processed information," but these two are in actual fact completely different. The difference lies in the fact that while "anonymously processed information" is information processed so that a specific individual cannot be identified, "pseudonymously processed information" is information processed so that a specific individual can be identified if collated with other information. In this regard, it should be noted that "personal information" is defined in the Act as information concerning a living individual which, alone or **by being readily collated with other information**, identifies a specific individual. As such, "pseudonymously processed information" could continue to fall under the definition of "personal information" if this information can be readily collated with other information to identify a specific individual, while "pseudonymously processed information" that can be collated but only with difficulty would not fall under the definition of "personal information". On the other hand, anonymously processed information, by definition, does not constitute "personal information" because anonymously processed information must have been processed to the extent that the individual is no longer identifiable, even if such information is collated with other information.

A database, etc. that is systematically structured so that it is possible to search pseudonymously processed information is defined as a "pseudonymously processed information database, etc." and a business operator that uses a pseudonymously processed information database, etc. for its business is defined as a "pseudonymously processed information handling business operator" (Article 2(10) of the

Amended Act).

Obligations concerning pseudonymously processed information

When a personal information handling business operator creates pseudonymously processed information that constitutes part of a pseudonymously processed information database, etc., it must do so in accordance with the method stipulated in the Enforcement Rules (to be established by the PPC at a future date), and it must also take necessary measures in accordance with the Enforcement Rules to prevent leakage of deleted or processed information (Article 35-2(1)-(2) of the Amended Act).

A pseudonymously processed information handling business operator that is also a personal information handling business operator shall not use pseudonymously processed information that falls under personal information for purposes other than the purposes specified in advance unless permitted by other laws and regulations (Article 35-2(3) of the Amended Act).

Furthermore, unless permitted by other laws and regulations, pseudonymously processed information must not be provided to a third party regardless of whether or not it falls under the scope of personal data. On the other hand, the provision of such information in connection with consignment, business succession and joint use will be permitted (Article 35-2(6), Article 35-3(1)-(2) of the Amended Act). As stated below re-identifying a principal from pseudonymously processed information is prohibited, so such information may not be provided to a third party even if consent is obtained from the principal.

A pseudonymously processed information handling business operator is prohibited from collating pseudonymously processed information with other information to identify the principal (Article 35-2(7), Article 35-3(3) of the Amended Act). It should be noted that while pseudonymously processed information is, by definition, information that may identify an individual when collated with other information, such collation is actually prohibited. Furthermore, it is prohibited to use any contact information contained in pseudonymously processed information to make a telephone call or to send an e-mail, physical mail, facsimile, or telegraph, etc., to a principal, or to visit a principal's home (Article 35-2(8), Article 35-3(3) of the Amended Act). As it can be understood from these provisions, pseudonymously processed information is not intended to be used to identify an individual, but is intended to be utilized as big data for the purposes of statistical market research or research on consumer trends inside a company.

Exemption from certain obligations concerning personal information or personal data

In exchange for the new obligations to ensure proper handling of pseudonymously processed information, the Amendment stipulates that even if pseudonymously processed information falls under the definition of personal information, personal data, or retained personal data, it is not subject to the restrictions on the extent that business operators can change the purposes of use of personal information (Article 15(2) of the Amended Act), the reporting of incidents where personal data is leaked,

lost or damaged (Article 22-2 of the Amended Act) or the right to demand for the disclosure, correction, addition, deletion, suspension of use or erasure of retained personal data (Article 27 to Article 34 of the Amended Act).

As mentioned above, some business operators have used masking as part of their security control measures. However, under the current Act, information that does not meet the standards for the creation of anonymously processed information as stipulated in the Enforcement Rules is not treated as anonymously processed information ("Q&A for the PPC's Guidelines (last updated on November 12, 2019)" Q11-4-2), and if one can identify an individual by easily collating such information with other information, such information will still be deemed to be personal data subject to a demand for disclosure, etc. The Amendment aims to reduce the burden on business operators when they have to respond to such demands, and to promote a more flexible utilization of such data that meets the definition of pseudonymously processed information.

The provisions obligating business operators to specify the purposes of use (Article 15(1) of the Amended Act) and the provisions obligating business operators to notify or disclose those specified purposes of use (Article 18 of the Amended Act) will continue to apply to pseudonymously processed information as long as such information also falls within the definition of personal information.

Preparation by the effective date

To our knowledge, many business operators have stipulated in their internal regulations the procedures, precautionary measures and rules in processing information on the basis of the distinction between personal information and anonymously processed information under the current Act. After the effective date of the Amendment, if business operators anticipate that they will be using pseudonymously processed information, it would be necessary for them to add new provisions to their internal regulations on the handling of pseudonymously processed information, as well as sufficiently educate their employees on this complicated regulatory structure under the Amended Act. Furthermore, because business operators must create and preserve pseudonymously processed information in accordance with the detailed rules in the Enforcement Rules to be established by the PPC, it would be necessary for them to establish appropriate operational procedures that are in line with the Enforcement Rules.

(5) Expansion of the scope of extraterritorial application

The 2015 Amendment introduced a provision on extraterritorial application for the first time in the history of the Act. That provision, which is currently still in effect, stipulates that only certain provisions in the Act concerning (i) the purposes of use of personal information, (ii) security control measures concerning personal data, (iii) third party provision of personal data (excluding the recipient's confirmation and recording obligations), (iv) disclosure of certain information on retained personal data and demands for disclosure, etc. of retained personal data, (v) creation of anonymously processed information, and (vi) advice, guidance and recommendations by the PPC (excluding demands for reports, on-site inspections and orders) apply to "cases where a personal information handling business operator,

who in relation to supplying a good or service to a person in Japan has acquired personal information relating to such person (where such person is a principal), handles the personal information or anonymously processed information produced by using the said personal information in a foreign country" (Article 75 of the Act). The Amendment expands the scope of the provision on extraterritorial application to cover the entire Amended Act, and replaces the stipulation on the cases to which the extraterritorial application provision applies with the following: "cases where a personal information handling business operator, etc.[8], in relation to supplying a good or service to a person in Japan, handles the personal information that has a person in Japan as the principal, personally referable information that is to be acquired as such personal information, pseudonymously processed information or anonymously processed information produced by using such personal information, in a foreign country" (Article 75 of the Amended Act). In other words, the requirement that the personal information has to be "acquired" in relation to supplying a good or service to a person in Japan has been deleted, and the new provision instead broadly covers situations where personal information, etc. is handled in relation to the supply of goods or services to a person in Japan, regardless of the relevance to Japan at the time of acquisition. In addition, personally referable information, though by itself not personal information, is subject to the provision on extraterritorial application if it is anticipated that a third party will acquire such personally referable information as personal information. With respect to enforcement by the PPC, the key point is that the provisions concerning the PPC's demands for reports, on-site inspections and orders could be extraterritorially applied after the effective date.

We will need to keep a close watch on the extent to which the PPC will enforce the Amended Act extraterritorially in practice. However, as a general rule, if the principal identified by personal information is located in Japan and if the business operator is conducting business in Japan, the provisions of the Amended Act will fully apply even in a foreign country.

(6) Strengthened enforcement power of the PPC and criminal penalties

Under the Amended Act, a new provision has been introduced to enable the PPC to disclose the names of business operators that breach the PPC's legally binding orders (Article 42(4) of the Amended Act). The PPC's actions are comprised of multiple levels of actions; i.e., advice and guidance, recommendations, and (legally binding) orders, and an order is the strongest of these actions that imposes a fine (Article 41 and Article 42 of the Amended Act. The PPC may also demand a report and conduct an on-site inspection where non-compliance is subject to a fine.). By expressly giving the PPC the ability to impose social sanctions by "naming and shaming" business operators who breach the PPC's orders by disclosing their names publicly, the PPC will have more effective powers of enforcement[9].

---

[8] In this context, "personal information handling business operator, etc." collectively refers to personal information handling business operators, personally referable information handling business operators, pseudonymously processed information handling business operators, and anonymously processed information handling business operators.

[9] As a cultural background, business entities (especially large companies) in Japan are keen to maintain a good reputation. Generally, this kind of social sanction is taken seriously by business entities and consumers in Japan, and a publication of the fact that a business entity has violated the Act would cause a serious reputational risk that would be likely to negatively affect the entire business of that entity. Therefore, this is expected to work as an effective deterrent to a violation of a PPC order.

As for criminal penalties, the maximum period of imprisonment for breaching the PPC's order has been increased from six months to one year, and the maximum fine has been raised from JPY 300,000 to JPY 1,000,000 (Article 84 of the Act, Article 83 of the Amended Act). The maximum fine for refusal to report or making a false report has been raised from JPY 300,000 to JPY 500,000 (Article 85 of the Act, Article 85 of the Amended Act). The penalty for the provision or theft of a personal information database, etc. that an individual has handled in business activities for the purpose of seeking illicit profits is imprisonment for not more than one year or a fine of not more than JPY 500,000, which remains the same under the Amended Act (Article 83 of the Act, Article 84 of the Amended Act).

Under the current Act, if a representative of a legal entity, or an agent, employee or other worker for a sole proprietor or legal entity commits a crime in connection with their business, such sole proprietor or legal entity is also subject to the same criminal penalties as the individual who committed the crime. Under the Amended Act, if a representative or agent, employee or other worker for a legal entity breaches the PPC's order or commits a crime of providing or stealing a personal information database, etc., the maximum fine imposed on the legal entity is JPY 100,000,000 (Article 87 of the Act, Article 87 of the Amended Act). In view of the discrepancy in financial power between legal entities and individuals, the fine has been significantly raised for legal entities in particular.

According to the System Reform Outline, the administrative monetary penalties are subject to continuous review, although this statement has not been included in the Amendment.

(7) Others

With respect to accredited personal information protection organizations, the Amendment introduces a system to enable the PPC to accredit an organization that covers/supervises only certain business units of personal information handling business operators (e.g. the financial unit of a personal information handling business operator) (Article 47(2) and Article 49-2 of the Amended Act). According to the System Reform Outline, the aim of this system is to utilize the professional knowledge of organizations that focus only on certain type(s) of businesses or industries and to promote the private sector's efforts to address personal information protection. Furthermore, if a business operator subject to the supervision of an accredited personal information protection organization continues to breach the organization's personal information protection policy, in spite of guidance and recommendation given by the organization, such business operator could be excluded from the coverage of the organization (Article 51, paragraph 1 of the Amended Act).

In addition, the Amendment has introduced some provisions stipulating that certain provisions in the Civil Procedures Act concerning service shall also apply to the process of issuing and delivering demands for reports, recommendations and orders by the PPC (Article 58-2 to Article 58-5 of the Amended Act).

3. Conclusion – Recap of necessary actions

At present, we do not have a comprehensive view of the entire system reform because the Amendment has delegated most of the practical and technical aspects to the PPC's Enforcement Rules which will only be established at a future date. However, it is already clear that the Amendment will have a substantial effect on the practice of handling personal information by business operators.

Business operators are advised to begin checking and determining which of their business practices would be affected by the Amendment, and make preparations to comply with the Amended Act when it comes into effect by taking the necessary preparatory steps such as revising their internal regulations and educating their employees well in advance. The PPC has publicized a draft roadmap for the smooth implementation of the Amended Act[10], which should serve as a useful reference for planning the necessary actions to deal with the changes brought about by the Amendment.

[10] Materials for the 144th meeting of the Commission, "The Personal Information Protection Commission's future actions in response to the approval of the Act on Partial Amendment of the Personal Information Protection Act (draft)" (June 15, 2020; https://www.ppc.go.jp/files/pdf/200615_shiryou1.pdf, available only in Japanese)

- This newsletter is published as a general service to clients and friends and does not constitute legal advice. Should you wish to receive further information or advice, please contact the authors as follows.

- Authors:
  Nobuhito Sawasaki（nobuhito.sawasaki@amt-law.com）
  Ryo Murakami（ryo.murakami@amt-law.com）

- If you wish to unsubscribe from future publications, kindly contact us at General Inquiry.
- Previous issues of our newsletters are available here.