"Is Your Company Prepared for the Implementation of the Personal Information Protection Act on April 1, 2022?"

Introduction

As countries around the world bolster their laws to protect the privacy of personal data and information, including the European Union's General Data Protection Regulation (GDPR), Japan has also taken a major step in strengthening its data protection laws to, in part, meet the stringent global standard set forth by the GDPR.

Japan's privacy act, the Personal Information Protection Act (PIPA), was amended on June 12, 2020 and will be made effective on April 1, 2022. The amendments were made to increase awareness of personal information, balance protection and utilization in light of technological innovation, and address new risks associated with the increased distribution of cross-border data. Enforcement regulations were also released on March 24, 2021 to also be made effective on April 1, 2022.

The key amendments that we believe will impact companies that do business in Japan and their foreign affiliated entities are related to: 1) the expansion of the definition of "retained" personal data; 2) disclosure requirements; 3) leakage reporting requirements; 4) new category of information called "personally-related information"; 5) cross-border transfers of personal data; 5) expansion of extraterritorial application; and 6) increased penalties for violations of the Act**.**

We believe that the effect of these amendments will be significant for those operating both domestically and internationally, and specific measures such as reconsidering business structures and revising privacy policies will be necessary. Therefore, with less than a month to go until the effective date of the amended law, this newsletter provides you with more details on the amendments than a typical newsletter as we would like more hands-on type advice. We have arranged the format in an easy-to-follow Q&A format which should guide you to the detailed information that you need. We have included a lot of details so that this newsletter can be a great resource for any privacy issues that involve the handling of personal information.[1]

---

[1] The Personal Information Protection Commission, Government of Japan is referred to as the "**Commission**"; the Personal Information Protection Act is referred to as the "**Act**; the Cabinet Order to Enforce the Act on the Personal Information Protection Act is referred to as the "**Cabinet Order**"; Enforcement Rules for the Personal Information Protection Act is referred to as the "**Enforcement Rules**"; the Guidelines for the Personal Information Protection Act (General Provisions) and other guidelines (Guidelines on the Personal Information Protection Act (Provision to Third Parties in Foreign Countries), Guidelines on the Personal Information Protection Act (Obligation to Confirm and Record when Providing to Third Parties), Guidelines on the Personal Information Protection Act

Expansion of the Definition of "Retained Personal Data"

Q1: Even for personal data[2] that has been deleted within a short period of time after acquisition, will there be an obligation to make the relevant matters public and to respond to requests for disclosure, correction, or suspension of use?

A1: A company[3] shall make the relevant matters public, and an individual as a data-subject is entitled to have his/her retained personal data[4] disclosed, corrected, suspended from use, etc., under the Act (please also see Q2 to Q4).

Prior to the amendments, the Act allowed any personal data that was to be deleted within six months of acquisition to NOT be considered "retained personal data" that would fall under the Act's requirements. However, the amendments removed this six-month qualification, basically making ANY personal data to be considered "retained personal data" regardless of their retention period.[5]

Indeed, the reasoning behind this change was due to the speed of the development of the flow of information, the increase in the risk of personal data instantly spreading and leaking, and the increase in the risk of infringement of the rights and interests of individuals.

The amendments to the Act have also created stricter rules for the disclosure of retained personal data since the company has authority to disclose and revise such data and the amendments aim to ensure that retained personal data is disclosed and handled properly.

Additional Items to be Disclosed by Companies Handling Personal Information

Q2: Has there been any change in the scope of matters regarding personal data that should be made public? What details about security control measures should be disclosed?

A2: Under the amended Act, items subject to public disclosure by companies have been added to enable individuals to be better aware of how their retained personal data is being handled. The specific items which were added through the amendment of the Act are (additional items are underlined):

(Pseudonymized Information and Anonymously Processed Information), Guidelines on the Personal Information Protection Act (Accredited Personal Information Protection Organizations) are referred to as the "**Guidelines**"; the Q&A regarding the "Guidelines for the Personal Information Protection Act " and the "Response to the Occurrence of a Personal Data Leakage or Other Incident" is referred to as the "**Q&A**". You may find these laws and guidelines in the following link in the Commission website: https://www.ppc.go.jp/personalinfo/legal/

[2] The term "personal data" refers to personal information that is included or used in a personal information database, etc. Article 16, Paragraph 3 of the Act. "Personal data" also includes "retained personal data".

[3] The term "company" refers to a private business operator that uses a personal information database, etc. for its business. Article 16, Paragraph 2 of the Act

[4] The term "retained personal data" refers to personal data for which a company has the authority to disclose, etc. (with some exceptions). Article 16, Paragraph 4 of the Act.

[5] Article 16, Paragraph 4 of the Act

1. The name and address of the company, and in the case of a corporation, the name of its representative; and
2. Measures taken for the security control of retained personal data (except for those measures where the disclosure may hinder the security controls)

The Guidelines on the Act provide examples of how security control measures should be disclosed to the public in each item as below.[6] However, as the content of a company's security control measures differs depending on how its business handles personal information, it is necessary to determine the content of the public announcement on a case-by-case basis.

- Formulation of Basic Policy
  In order to ensure the proper handling of personal data, a basic policy has been formulated regarding "compliance with related laws and guidelines", "contact points for questions and complaints", etc.

- Establishment of Rules for the handling of personal data
  Personal data handling rules are established for each stage of acquisition, use, storage, provision, deletion and disposal, with regard to handling methods, responsible parties and persons in charge and their duties.

- Organizational Security Control Measures
  A person in charge of handling personal data is appointed, the scope of employees handling personal data and the scope of personal data handled by such employees are clarified, and a reporting and communication system to the responsible person is established in the event that facts or signs of violations of the law or handling regulations are detected.

- Human Security Control Measures
  Periodic training is provided to employees on precautions regarding the handling of personal data and matters regarding confidentiality of personal data are included in the company's employment rules.

- Physical Security Control Measures
  In the area where personal data is handled, access and control measures of employees and restrictions on equipment brought into the area are implemented, and measures are taken to prevent unauthorized persons from viewing personal data. Measures are also taken to prevent theft or loss of equipment, electronic devices, and documents that handle personal data, and measures are taken to prevent personal data from being easily identified when such equipment and electronic devices are transported, including within the business premises.

- Technical Security Control Measures
  Access control is implemented to limit the scope of the person in charge and the personal information database to be handled. A system is implemented to protect information systems that handle personal data from unauthorized access from outside or unauthorized software.

[6] Guidelines (General Provisions) 3-8-1

- Understanding the external environment
  Security control measures are implemented based on an understanding of the system for the protection of personal information in Country A, where personal data is stored.

With regard to the method of public disclosure, a company is permitted to post an outline or part of the measures taken on the website, establish a contact point for inquiries, and be ready to respond orally or in writing to any inquiries.[7]

However, for example, it is not appropriate to only post or answer that the company is implementing safety control measures in accordance with the "Guidelines for the Personal Information Protection Act (General Provisions)."[8] Therefore, it is necessary for you to prepare to post appropriate content or respond appropriate answers without delay.

Methods of Disclosure

Q3: How should retained personal data be disclosed? Has it become easier for the individual to request disclosure of records of the company's provision of personal data to third parties?

A3: Under the Act prior to the amendment, when a request was made for the disclosure of retained personal data, the disclosure had to be made in writing or by a method agreed to by the individual making the request.[9] However, the amended Act now allows the individual to specify the method of disclosure to the company to a certain extent.[10] Therefore, in the future, if a method of disclosure other than the one proposed by the company is specified by the individual, the company must, in principle, respond to the individual's request.

In addition, companies handling personal information are obliged to record relevant matters when providing or receiving personal data to a third party[11], and in the Act prior to the amendment, such records were subject to disclosure only when they fell under the category of "retained" personal data. However, under the amended Act, records provided to third parties are subject to disclosure in addition to retained personal data.

Q4: Has it become easier for the individual to request the suspension of use, deletion, or suspension of provision by the company to a third party of retained personal data? In what cases can a request be refused?

A4: Under the Act prior to the amendment, requests by the individual to the company for the suspension of use or deletion of retained personal data were limited to cases where there was a violation of the Act by the company, such as when personal information was obtained illegally. Also, requests for the suspension of provision by the company to a third party were allowed only in cases where there was a violation of the Act by the company, such as when the consent of the individual was not obtained in advance.[12] However, under the amended

---

[7] Guidelines (General Provisions) 3-8-1 *1
[8] Guidelines (General Provisions) 3-8-1 (4)
[9] Article 28, Paragraph 2 of the Act prior to the amendment and Article 9 of the Cabinet Order
[10] Article 33, Paragraph 1 and Paragraph 2 of the Act
[11] Article 29, Paragraph 1 and Article 30, Paragraph 3 of the Act
[12] Article 30, Paragraph 1 and Paragraph 3 of the Act prior to the amendment (Article 35, Paragraph 1 and Paragraph 3 of the Act after the amendment)

Act, in addition to these cases, requests for the suspension of use, deletion, or suspension of provision to a third party can now be made in the following cases:[13]

1. When there is no longer a need for the company to use the retained personal data that identifies the individual;
2. When a situation such as a leak relating to the retained personal data that identifies the individual has occurred (limited to a situation subject to reporting in A5); or
3. When there is a risk that the rights or legitimate interests of the individual will be harmed by the handling of the retained personal data that identifies the individual.[14]

In response to such a request, the company can refuse the request where the suspension of use of the retained personal data will be costly, or where it is difficult to suspend the use and the company takes alternative measures necessary to protect the rights and interests of the individual.[15]

The following cases are listed in the Guidelines[16] as possible alternative measures necessary to protect the rights and interests of the individual:

1. A case in which a promise is made to correct a list of names at the time of its reprinting and the reprinting and collection of a list of names that is already on the market will be costly.
2. A case in which a serious leak subject to a report to the Commission has occurred, and because the contract with the individual is still in effect, it is difficult to suspend the use, and necessary and appropriate measures are taken to prevent the recurrence of the leak in the future.
3. A case in which, instead of deleting without delay retained personal data that is required to be retained under other laws and regulations, the company promises to delete the data after the end of the retention period under such laws and regulations.

Responses to and Reports of Data Leakage

Q5: Has the company's response to data leakage been made stricter?

A5: Yes, prior to the amendment, a company only had the obligation to make best efforts to report to the Commission that a leak, loss, or damage of personal data occurred or was likely to occur ("**Leakage**").[17] However, under the amended Act, companies now have the obligation to report to the Commission any "situations that pose a significant risk of harm to the rights and interests of an individual" when a Leakage is discovered, and to notify the individual of the occurrence of such a situation.[18]

---

[13] Article 35, Paragraph 5 of the Act

[14] Cases in which the sending of direct mail or telemarketing is repeated against the individual's will, etc. Guidelines (General Provisions) 3-8-5-1 (3)

[15] Article 35, Paragraph 6 of the Act

[16] Guidelines (General Provisions) 3-8-5-3

[17] "How to Respond in the Event of a Leakage of Personal Data" (Personal Information Protection Commission Notice No. 1 of 2017)
https://www.ppc.go.jp/personalinfo/legal/leakAction/leakAction_detail/

[18] Article 26, Paragraph 1 and Paragraph 2 of the Act

The Enforcement Rules[19] provide some examples of such "situations that pose a significant risk of harm to the rights and interests of an individual":

1. Leakage of personal data that contains special care-required personal information[20]
2. Leakage of personal data that is likely to cause property damage if used inappropriately[21]
3. Leakage of personal data that is likely to be used for wrongful purposes[22]
4. Leakage in which the number of individuals as data-subject exceeds 1,000

In addition, the measures to be taken by companies in the event of the discovery of other Leakage have also been changed from a best-efforts obligation to a legal requirement.[23]

Thus, in the event that a Leakage is discovered in the future, companies will be required to respond without fail in accordance with the amended Act.

Q6: Who is required to report personal data leaks to the Commission and notify the individual, and how?

A6:

1. Who is to report and notify Leakage?

The entity that is obligated to report and notify a Leakage is the company that handles the personal data. However, a company to whom all or part of the handling of personal data is outsourced is exempted from the obligation to report and notify if it notifies the company which outsourced the handling of personal data of the Leakage.[24]

2. Report to the Commission[25]

Reports of Leakage are divided into two stages: 1) a preliminary report; and 2) a final report.[26] A preliminary report must be made promptly (generally within 3 to 5 days) after discovering the occurrence of a Leakage, and a final report must be made within 30 days (60 days in the case where there is leakage of personal data that is likely to be used for wrongful purposes).[27]

The items to be reported are: 1) an outline of the Leakage; 2) the items of personal data that have been or may have been leaked; 3) the number of individuals as data-subject that have been or may have been leaked; 4) the cause of the Leakage; 5) the existence of any ancillary damages or the possibility of ancillary damages and details thereof; 6) the status of implementation of response to the individual; 7) the status of implementation of a public announcement; 8) measures to prevent a recurrence; and 9) other helpful items. In principle,

---

[19] Article 7 of the Enforcement Rules

[20] Information on medical treatment and medicine dispensing of patients in hospitals, and results of medical examinations, etc. of employees. Guidelines (General Provisions) 3-5-3-1

[21] Personal data including credit card numbers, personal data including combinations of login IDs and passwords for web services with remittance and payment functions, etc. Guidelines (General Provisions) 3-5-3-1

[22] Cases in which personal data has been leaked due to unauthorized access, and cases in which an employee has illegally taken a customer's personal data and provided it to a third party. Guidelines (General Provisions) 3-5-3-1

[23] Guidelines (General Provisions) 3-5-2

[24] Article 26, Paragraph 1, Proviso, and Paragraph 2, Main text, Parentheses of the Act

[25] Article 26, Paragraph 1 of the Act

[26] Article 8 of the Enforcement Rules

[27] Article 8, Paragraph 2 of the Enforcement Rules

the report should be submitted by filling in the report form on the Commission's website.[28] As for the contents of the report at the time of the preliminary report, it is sufficient to report the contents that are known at the time of the report.

3. Notification to the individual[29]

On the other hand, with regard to notification to the individual, when a company becomes aware of a leakage situation subject to reporting under A5, the company must promptly notify the individual in accordance with the circumstances of the situation. However, if it is difficult to notify the individual, the company is allowed to take alternative measures necessary to protect the rights and interests of the individual.[30]

The items to be notified to the individual are: 1) an outline of the Leakage; 2) the items of personal data that have been or may have been leaked; 3) the cause of the Leakage; 4) the existence of any ancillary damages or the possibility of ancillary damages and details thereof; and 5) other helpful items[31]. As for the means of notification, the Guidelines provide for notification by sending a document by postal mail or e-mail[32].

New Category of Information called "Personally-Related Information"

Q7: What is personally-related information? Please tell us if there are any obligations that we should observe when handling it.

A7: Prior to the amendments, it was not clear on the obligations of a company that transferred information in which the receiving party is the only party who could identify the individual. The amended Act attempted to add protection for this type of information by creating a new category of information called "personally-related information". Under the amended Act, personally-related information is defined as "information relating to a living individual that does not fall under any of the categories of personal information, pseudonymized information, or anonymously processed information." [33] Although this definition is quite broad, the Guidelines have provided examples of personally-related information such as an individual's website browsing history collected through cookies, and other terminal identifiers, as well as an individual's age, gender, family structure, etc., which are linked to an individual's email address.[34]

For such information, if a company provides it to a third party and (1) assumes that the information will be obtained as personal data by the party to which it is provided, (2) intends to provide personally-related information as part of the company's personally-related information database to a third-party,[35] the company shall not, in principle, provide such information without confirming that consent of the individual as data-subject has been

---

[28] Article 8, Paragraph 1 of the Enforcement Rules, and Guidelines (General Provisions) 3-5-3-3
[29] Article 26, Paragraph 2 of the Act
[30] Publication of the case, preparation of a contact point and publication of the contact information so that the individual can confirm whether or not his or her personal data is the subject of the case, etc. Guidelines (General Provisions) 3-5-4-5
[31] Article 10 of the Enforcement Rules
[32] Guidelines (General Provisions) 3-5-4-4
[33] Article 2, Paragraph 7 of the Act
[34] Guidelines (General Provisions) 2-8
[35] Article 16, Paragraph 7 of the Act

obtained.[36] In addition, when confirming that consent has been obtained, in order to ensure the traceability of the personally-related information, the company is obliged to prepare a record of the relevant matters[37] as well as a record of the provision of the information to a third party, and retain it for a prescribed period of time.[38]

Companies that have treated such information as not falling under the category of personal information needs to be careful in the future.[39]

Q8: Who will obtain the consent of the individual and how will it be obtained for the provision of personally-related information to a third party? If the third-party recipient obtains the consent, how does the provider confirm such consent?

A8: The entity that typically obtains the consent is the third-party recipient, who has contact with the individual and uses the information, but the company provider of the personally-related information is allowed to obtain consent on behalf of the recipient, provided that the rights and interests of the individual are equally protected.[40]

For each case, it is necessary to make it possible for the individual to recognize the entity to whom the personally-related information is provided, the items of personally-related information to be covered, and the purpose of utilization after the personally-related information is provided.[41]

If the third party recipient obtains the consent, the company providing the personally-related information must confirm whether the third party has obtained the consent of the individual by receiving a declaration from the third party to whom the personally-related information is provided or by other appropriate methods.[42] At this time, it is sufficient for the company to generally confirm the contents of the declaration,[43] and it is not necessary to independently investigate whether consent has been obtained, unless there are special circumstances.

Q9: Please tell us what we should pay special attention to when we provide personally-related information to a third party in a foreign country.

A9: When providing personally-related information to a third party in a foreign country, a company handling personally-related information must, in addition to confirming that the consent of the individual has been obtained (*see* A7), confirm that the individual has been provided with the name of the foreign country, the system for protecting personal information in the foreign country obtained by an appropriate and reasonable method, and the information on the measures taken by the third party to protect personal information, at the time the consent is obtained[44].

---

[36] Article 31, Paragraph 1 of the Act

[37] Article 31, Paragraph 3 and Article 30, Paragraph 3 of the Act

[38] Article 31, Paragraph 3 and Article 30, Paragraph 4 of the Act

[39] Please see Article 5 of the Supplementary Provisions of the Act for transitional measures.

[40] Guidelines (General Provisions) 3-7-2-2

[41] Guidelines (General Provisions) 3-7-2-2

[42] Article 26, Paragraph 1 of the Enforcement Rules

[43] Guidelines (General Provisions) 3-7-3-1

[44] Article 31, Paragraph 1, Item 2 of the Act and Article 17, Paragraph 2 of the Enforcement Rules

However, if the recipient is located in the EU or the UK, or is a so-called standard-compliant system provider, it does not fall under the category of "a third party in foreign country"[45] and such confirmation is not required.

In addition, if the recipient is a standard-compliant system provider, necessary actions to ensure the continuous implementation of equivalent actions should be taken by the recipient.[46]

Additional Information that Companies Have to Disclose for Cross-Border Transfers of Personal Data

Q10: Please tell us about the new information that should be provided in the future when personal data is transferred across borders. In this case, are there any materials that summarize the outline of foreign personal information protection systems that companies can refer to?

A10: When a company provides personal data to a third party in a foreign country[47], it is necessary to obtain the prior consent of the individual for the "approval of provision to a third party in a foreign country", except when the third party is located in the EU or the UK, or is considered a "standard-compliant system provider".

In obtaining such consent, under the Act prior to the amendment, it was necessary to make it clear to the individual that the information was being provided to a third party in a foreign country, but it was not necessary to provide information on the name of the foreign country or the system for protecting personal information in that foreign country.[48]

However, in light of recent changes in the risks associated with cross-border transfers of personal data, such as the expansion of data protection legislation around the world, the provision of information to individuals is now required under the amended Act as follows:

1. When providing personal data to a third party in a foreign country and obtaining the consent of the individual, a company must, in advance, provide the individual with the name of the foreign country, information on the system for protecting personal information in the foreign country that obtained the personal data by appropriate and reasonable methods, and information on the measures taken by the third party to protect personal information.[49]
2. In the event that a company has provided personal data to a third party in a foreign country that is a "standard-compliant system provider", the company must take the necessary actions to ensure the continual implementation of reasonable actions by the third party (i.e., a standard-compliant system provider)[50], and provide the individual with information regarding the necessary actions[51] upon the individual's request.[52]

---

[45] Article 28, Paragraph 1 of the Act

[46] Article 31, Paragraph 2 and Article 28, Paragraph 3 of the Act

[47] This includes the case where a foreign company provides the information to a third party in the same country (Q12-7 of the Q&A). Please see Q13 for extraterritorial application.

[48] Q9-2 of the Q&A prior to the amendment

[49] Article 28, Paragraph 1 and Paragraph 2 of the Act and Article 17, Paragraph 2 of the Enforcement Rules

[50] Article 18, Paragraph 1 of the Enforcement Rules

[51] Article 18, Paragraph 3 of the Enforcement Rules

[52] Article 28, Paragraph 1 and Paragraph 3 of the Act

In this regard, the Commission has disclosed the results of a survey of foreign country systems for the protection of personal information, which may be a helpful reference in obtaining information on foreign systems:

https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#gaikoku.

In addition, the obligation to provide information will not be retroactively imposed on cases where the consent of the individual has already been obtained prior to the effective date of the amended Act, or where personal data has been provided to a recipient who is a standard-compliant system provider.[53]

Q11: Please tell us about the new information that should be provided going forward when personal data is stored on a server using a cloud service provided by a foreign business entity.

A11: If the operator of the server of the cloud service does not handle personal data stored on the server, the act of the company storing personal data on the server does not constitute "provision to a third party in a foreign country" and there is no need to obtain consent from the individual.[54]

In such case, the company is deemed as handling personal data by itself abroad. Regardless of the country where the server is located, -- e.g., a company that operates a server is located in Germany and the server is located in either Japan or Italy --the company handling personal information needs to understand the foreign country's systems in protecting personal information, and take the necessary security control measures.[55] In accordance with the amended Act, the company handling personal information is required to make public the details of such measures as well as the name of the country where the operator of the server is located (and the country where the server is located if the server is located in a foreign country)[56] (*see* A2).

On the other hand, if a server operator handles personal data and the act of storing personal data on the server falls under "provision to a third party in a foreign country", the information that the company should provide to the individual in accordance with the amended Act (*see* A9) is not the information of the foreign country where the server is located, but the information of the foreign country where the server operator is registered as a legal entity.

In addition, if the country where the server is or will be located is known, the Q&A recommends providing the individual with information on the system of such country from the viewpoint of ensuring accountability and transparency to the individual.[57]

Expansion of Extraterritorial Application

Q12: What kind of cases are covered by the extraterritorial application?

---

[53] Article 4 of the Supplementary Provisions of the Act

[54] Q12-3 of the Q&A

[55] Article 23 of the Act

[56] Q10-25 of the Q&A

[57] "Question and Answer: 2020 Amendment to the Personal Information Protection Act" (the "**Planners' Commentary**") Q48, Kiyoshi Sawaki (ed.), and Q12-11 of the Q&A

A12: The amended Act expands the scope of the extraterritorial application of the Act and fully permits the extraterritorial application of the Act where a company in a foreign country handles the personal information of a person residing in Japan in connection with the provision of goods or services.[58] For this reason, the Act applies not only to cases where a foreign company directly acquires personal information from an individual in Japan, but also to cases where it is indirectly acquired from another company in Japan.

The following cases are listed in the Guidelines as examples of cases subject to extraterritorial application. [59]

1. When a foreign internet mail order business handles personal information of Japanese consumers in connection with the sale and delivery of products to them.
2. When a foreign hotel operator handles personal information of Japanese consumers provided by a travel agency in Japan in connection with the provision of services such as the distribution of information on local sightseeing spots and events to Japanese consumers.
3. When a foreign advertising-related company provides a Japanese internet mail order company with personal information that is expected to be linked to the personal data of Japanese consumers held by the internet mail order company in connection with the provision of services such as the distribution of campaign information to Japanese consumers by the internet mail order company.
4. When a foreign application provider handles pseudonymized information created using the personal information of Japanese consumers to develop new services in connection with the provision of services to Japanese consumers.
5. When a foreign internet mail order company handles anonymously processed information created using the personal information of Japanese consumers to conduct trend analysis in connection with the sale of products or provision of services to Japanese consumers.

In addition, the following case is listed in the Guidelines as an example of case that is NOT subject to extraterritorial application. [60]

1. When a parent company located in a foreign country handles personal information of the employees of a subsidiary company located in Japan for the purpose of managing employee information of the group company.

In addition, a foreign company handling personal information that is subject to the extraterritorial application of the Act must take security control measures for personal data based on an understanding of the systems relating to the protection of personal information in the foreign country where the personal data is handled.[61] Also, the name of the foreign country and the details of such measures must be made public.[62]

Q13: Is it now possible to collect reports and give orders to foreign companies? What measures will be taken if the Commission's order is not complied with?

---

[58] Article 166 of the Act, however, some penalty provisions are excluded (Article 178 of the Act)
[59] Guidelines (General Provisions) 8
[60] Guidelines (General Provisions) 8
[61] Article 23 of the Act
[62] Q11-2 of the Q&A

A13: Under the Act prior to the amendment, the Commission's authority over foreign companies was limited to guidance, advice and recommendations.

In contrast, the amended Act makes it possible for the Commission to collect reports and give orders to foreign companies.[63] In addition, the amended Act clearly states that if a company violates an order of the Commission, the Commission may make a public announcement to that effect.[64]

The Commission's need to publicize the violations of orders is expected to be particularly high for foreign companies subject to the extraterritorial application of the Act, as it is difficult to exercise supervisory authority and enforcement of the Act over such companies which are located in a different jurisdiction.[65]

Therefore, foreign companies who have not taken sufficient measures to comply with the Act so far need to be careful in the future.

Increased Penalties

Q14: Please explain the penalties for violations of the Act.

A14: The amended Act raises the statutory penalties to the same level as other similar economic offenses and provides for heavier fines for legal entities than for individuals as statutory penalties. For a comparison of the statutory penalties between the Act prior to amendment and the amended Act, please refer to the following (the amounts in red are those that have been amended).[66] Please note that this amendment has already come into effect as of December 12, 2020 and is applicable to acts committed on or after that date.[67]

		Imprisonment		Fine Amount	
		Before amendment	**After amendment**	**Before amendment**	**After amendment**
Violation of an order from the Commission	Individual	Less than 6 months	**Less than 1 year**	Less than 300,000 yen	**Less than 1 million yen**
	Corporations	-	-	Less than 300,000 yen	**Less than 100 million yen**
Unauthorized provision of personal information database	Individual	Less than 1 year	Less than 1 year	Less than 500,000 yen	Less than 500,000 yen
	Corporations	-	-	Less than 500,000 yen	**Less than 100 million yen**
False reports to the Commission	Individual	-	-	Less than 300,000 yen	**Less than 500,000 yen**

[63] Article 166, Article 143, Article 145, Paragraph 2 and Paragraph 3 of the Act
[64] Article 145, Paragraph 4 of the Act
[65] The Planners' Commentary Q86
[66] Of these, the unauthorized provision of personal information databases, etc. is also applicable to foreign companies (Article 178 and Article 174 of the Act).
[67] Article 8 of the Supplementary Provisions of the Act

		Imprisonment		Fine Amount	
		Before amendment	After amendment	Before amendment	After amendment
	Corporations	-	-	Less than 300,000 yen	**Less than 500,000 yen**

(Source: https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#houteikei)

Concluding Remarks

As mentioned above, the 2020 amendments to the Act will have a significant impact on businesses. Due to the limitation of space, this newsletter cannot comprehensively explain the background of the amendment, the detailed contents of the amended Act, and the details of the items indicated in the guidelines, etc. However, we believe it is important to grasp the outline of the amended Act and identify the points that need to be addressed by your company and the points that require further consideration. The Act will continue to be amended periodically in line with the remarkable progress of ICT. The 2020 amendments to the Act are one such example, and it is the responsibility of all companies that handle personal information to periodically monitor these amendments and take appropriate action on a case-by-case basis.

(Published March 1, 2022)

****

Sonderhoff & Einsel Law and Patent Office routinely provides legal advice related to data-related regulation, including the Act, public comments, compliance, contract drafting and amendment, negotiations, employee training, response to authorities, litigation and arbitration, and other related legal service.

The information provided in this document is only general information and does not provide specific professional advice. The views expressed in this newsletter are a personal one of the author and do not constitute a legal opinion of the firm. For inquiries, please contact Kengo Sakai and Yu Maruyama, the authors of this newsletter at: sakai@se1910.com, y-maruyama@se1910.com

****

Sonderhoff & Einsel Law and Patent Office
100-0005 1-6-2 Marunouchi, Chiyoda-ku, Tokyo
Shin-Marunouchi Center Building 18th Floor
http://se1910.com/

Tel +81-3-5220-6500
Fax +81-3-5220-6583