[Tentative Translation]

Act on the Protection of Personal Information
"The Every-Three-Year Review"
Outline of the System Reform

December 13, 2019

Personal Information Protection Commission

NOTICE

※ This paper is a provisional translation and may be subject to change. Please refer to the original version in Japanese for nuance.

[Tentative Translation]

Table of Contents

Chapter 1 Introduction 4
Chapter 2 Background of the Review 6
Chapter 3 Individual Matters 8
Section 1 Perspectives on Individual Rights regarding Personal Data 8
1. Basic Approach 8
2. Enhancement of the Inquiry Line for the APPI 8
3. Easing Requirements regarding Demands to Cease Utilization, Delete, and Cease Provision to a Third Party 9
4. Enhancement of the Right of Disclosure 10
5. Extending the Scope of Retained Personal Data to be subject to Demand for Disclosure etc. 12
6. Strengthening the Opt-Out Regulation 13
Section 2 Perspectives on Obligations that Business Operators Should Abide by 17
1. Mandatory Reporting of an Incident including a Leakage of Personal Data to the PPC and Notification of Such Incident to a Principal 17
2. Clarification of the Obligation for Proper Utilization of Personal Information 19
Section 3 Perspectives on Frameworks to Encourage Voluntary Activities of Business Operators 21
1. Accredited Personal Information Protection Organization System 21
2. Promotion of Voluntary Efforts by the Private Sector 23
Section 4 Perspectives on Policies for Data Utilization 25
1. Anonymously Processed Information System 25
2. Introducing "Pseudonymised Information (tentative name)" 25
3. Clarification of Exception Provisions regarding the Handling of Personal Information for Public Interest Purposes 26
4. Handling of Device Identifiers 27
5. Enhancement of Consultations on Utilization of Personal Information taking into account Its Protection and Utility. 30
6. Necessity of International Efforts for Data Utilization. 30
Section 5 Perspectives on Penalties 32
Section 6 Perspectives on Extraterritorial Application of the APPI and Perspectives on Efforts for International System Harmonization and Cross-Border Transfer 34
1. Basic Approach 34
2. Expansion of Scope of Extraterritorial Application 34
3. Reinforcement of Restrictions of Provision of Personal Data to a Foreign Third Party 36

[Tentative Translation]

Section 7 Handling of Personal Information by Public and Private Sectors 38
1. Basic Approach 38
2. Consolidation of Legal Systems relating to Administrative Organs and Incorporated Administrative Agencies and Legal Systems relating to the Private Sector 38
3. Personal Information Protection System of Local Public Entities 39
Section 8 Issue under Continuous Consideration 40
(Surcharge System) 40

[Tentative Translation]

[Legend]

2015 Amendment Act	Act on Partial Revision of the Act on the Protection of Personal Information and Act on the Use of Numbers to Identify a Specific Individuals in the Administrative Procedures (Act No. 65 of 2015)
PPC	Personal Information Protection Commission
APPI	Act on the Protection of Personal Information (Act No. 57 of 2003)
GDPR	The General Data Protection Regulation, established by the EU in April 2016. The regulation that took effect on May 25, 2018 as the law prescribing the protection of personal data in the EU, in replacement of the former Data Protection Directive 95 which was enforced in 1995.
Interim Summary	Interim Summary of Considerations in the Act on the Protection of Personal Information Every-Three-Year Review (publicly announced on April 25, 2019)

[Tentative Translation]

Chapter 1 Introduction

○ In light of the social and economic changes after the establishment of the 2015 Amendment Act, the Personal Information Protection Commission (PPC) has conducted "the Every-Three-Year Review", based on the "Perspectives in Discussions on the Every-Three-Year Review" that was published on January 28, 2019.

○ Although each perspective has variety of points of discussion, in the overall picture, there are common points of view. Such points of view were summarized in the Interim Summary. The following are current common points of view that were updated based on discussions and issues that occurred after the public announcement of the Interim Summary.

○ First, individuals providing their information are showing increasing interest and expectation toward involvement in handling of their own information by business operators. The system needs to be reviewed while taking heed of taking measures that are necessary and sufficient to ensure the "protection of an individual's rights and interests" specified in Article 1 of the Act on the Protection of Personal Information (APPI), which prescribes the purpose of APPI.

○ Second, the necessity to balance protection and use of personal information, which was especially emphasized in the 2015 Amendment Act, is still essential. It is important to aim for the system where technological innovation associated with personal information or information relating to an individual contribute to both economic growth and the protection of an individual's rights.

○ Third, various kinds of utilization of digitalized personal information is globally conducted. The system needs to be reviewed while considering to ensure international harmonization and coordination among systems.

○ Fourth, the use of services provided by foreign business operators and the businesses that handle personal information across national borders are increasing, and thus risks that an individual could face are changing. The system needs to accommodate such changes.

○ Fifth, as we embark on the age of AI and big data and the utilization of personal information further diversifies, it is becoming difficult for a principal to have a comprehensive prior understanding of how his or her own personal information will be handled. Under such circumstances, it is important to develop an environment

where business operators fulfill their accountabilities in terms of a principal’s rights and interests when handling personal information and properly use the information to the extent that the principal can predict.

○ For revising the system, in light of the fact that the technological and societal aspects of personal information are rapidly changing, a framework that enables flexibility is preferred. Additionally, in order to promote the creation of new industries, it is necessary to have business operators themselves proactively engage in efforts of personal information protection in a manner that suits their actual businesses, and it is important that such voluntary efforts and the system based on laws and regulations help realize a vibrant economic society and fulfilling citizens' lives.

[Tentative Translation]

Chapter 2 Background of the Review

○ The APPI was originally established in 2003 (fully enforced in 2005) and was amended in 2015, and the 2015 Amendment Act was fully enforced on May 30, 2017. In particular, in light of significant advancements in information and communications technologies, the 2015 Amendment Act included provisions to review the system every three years.

○ Based on Paragraph 3 of Article 12 of the Supplementary Provisions of the 2015 Amendment Act, every three years after the Act is enforced, the government is to review international trends in personal information protection, the advancement of information and communications technologies, the creation and advancement of new industries using personal information, to discuss the status on enforcement of the amended APPI after the 2015 Amendment Act (Amended APPI), and to take measures based on the results of the discussion if deemed necessary.

○ Additionally, based on Paragraph 2 of the same Article, after three year of the enforcement of the Amended APPI as a guide, the government is to review the status on the establishment of personnel structures, securement of funding and other measures necessary to effectively administer jurisdictional affairs of the PPC such as those related to the formulation and promotion of the Basic Policy on the Protection of Personal Information and others, to consider improvements in any of them, and to take measures based on the results if deemed necessary.

○ Furthermore, based on Paragraph 6 of the same Article, in light of statuses on enforcement of the Amended APPI, the execution of measures in Paragraph 1 and other matters, the government is to consider aggregating provisions regarding the protection of personal information which is defined in Article 2, Paragraph 1 of the Amended APPI and personal information retained by government agencies, and hence to consider how the system regarding personal information protection should be, including potential integral provisions.

○ In light of provisions in Article 12 of the Supplementary Provisions of the 2015 Amendment Act, the PPC has been conducting the Every-Three-Year Review. "Concluding the First Term of the PPC" was publicly announced at the 83rd meeting of the PPC (held on December 17, 2018). At the occasion of the end of the first term of the PPC under the leadership of then-Chairman, the document was published to hand over the experience in the past five years and main points of discussions based

on circumstances at the time to the next-term PPC.[1] In light of this, the "Focuses in Discussions on the Every-Three-Year Review" was publicly announced at the 86th meeting of the PPC (held on January 28, 2019).

○ In light of all of this, the PPC had analyzed and organized status of domestic and foreign policies, technologies and industries, and opinions of consumers regarding personal information protection. In addition, the PPC interviewed representatives of industrial associations. As a result, the PPC publicly announced the Interim Summary on April 25, 2019.

○ Then the PPC sought public comments on the Interim Summary from April 25 to May 27, 2019. Totally 525 comments were submitted by a total of 137 organizations, business operators and individuals.

○ While considering opinions gathered by the public comment procedure, the PPC has contemplated in-depth by interviewing and engaging in other activities to understand actual circumstances (deliberated a total of 24 times at the PPC meetings), and hence organized this "The Every-Three-Year Review Outline of the System Reform". The PPC will seek public comments once again, on the Outline this time.

○ The PPC is going to draft a bill, if legislative measures are needed, and aim to submit the bill to revise the APPI at the regular Diet session in 2020 based on the result of the public comment procedure on the Outline and other considerations.

○ With regard to the timing to enforce the Amendment Act, it will be put into effect after a certain preparation period so that business operators can appropriately prepare for the Amendment Act.

○ When enforcing the Amendment Act, the PPC will strive to communicate the new system to public and enable smooth transition while leveraging private sector's efforts in the current system.

[1] From the establishment of the Specific Personal Information Protection Commission on January 1, 2014 to December 31, 2018.

[Tentative Translation]

Chapter 3 Individual Matters

Section 1 Perspectives on Individual Rights regarding Personal Data

1. Basic Approach

○ This is an important topic for both individuals and business operators who use personal data, and careful and detailed discussions are required based on effectiveness, actual circumstances and effects. Especially, comments gathered through the Inquiry Line for APPI (Inquiry Line) or interviews show that opinions differ between consumers and business operators in many points and multidimensional discussions are required. Large differences were seen in general in the public comments for the Interim Summary.

○ The APPI is compatible with the eight basic principles of the Privacy Guidelines by the Organization for Economic Co-operation and Development (OECD), and the provisions on individual rights on personal data is in harmony with international standards. However, with regard to a principal's involvement, complaints regarding the handling of personal information by business operators received through the Inquiry Line were not only toward respective business operators but also toward the system, and therefore, the PPC focused on the topic.

2. Enhancement of the Inquiry Line for the APPI

○ The Inquiry Line was established, upon centralization of authorities in supervising on personal information to the PPC after the 2015 Amendment Act.

○ The PPC has recognized the importance of the Inquiry Line as a touchpoint with consumers and business operators. With regard to cases for which consultations were received, the PPC strive to attend in an attentive manner to satisfy consumers and others as much as possible, and it is important to steadily proceed with this effort going forward. Additionally, there have been cases where information received through the Inquiry Line led to guidance on the handling of personal information, and thus, the Inquiry Line is also important in collecting information for supervision operations.

○ Furthermore, with regard to mediation of complaints, the PPC has led to resolving stagnant cases between consumers and business operators, and the PPC considers that a certain level of results are achieved. The PPC needs to steadily proceed with this effort. Thus, it is important to proactively inform the complaints mediation system to consumers who show complaints about business operators' handling of personal information.

○ In the public comments for the Interim Summary, the PPC received opinions requesting that the Inquiry Line be operated in a manner in line with actual operations of business operators and with further convenience. Going forward, efforts will be made to further fulfill the Inquiry Line's services, such as engaging in activities to further enhance the satisfaction of consultees by continuing to respond attentively and introducing the AI-based chatbot (a 24-hour service that can automatically respond to frequent and relatively simple questions) in order to enhance convenience for citizens.

○ With regard to consultations received through the Inquiry Line or chatbot, they shall be aggregated as valuable opinions, with anonymity retained, and the content of frequent topics are to be presented in an easy-to-understand manner in the form of guidelines or Q&A. Additionally, tendencies in consultations will be analyzed so that services will be further enhanced to enable consultations in a manner that is detailed and meets the interests or needs of consultees.

3. Easing Requirements regarding Demands to Cease Utilization, Delete, and Cease Provision to a Third Party

○ With regard to cease of utilization and deletion, as demonstrated in the Interim Summary, opinions received through the Inquiry Line and discussions at town meetings show that consumers are very dissatisfied when business operators do not cease the utilization of or delete their personal information.[2] However, in light of the fact that there are cases where some of the business operators attend to customers' demands to cease utilization, which meets the criteria of "JIS[3] Q 15001 Personal Information Protection Management System – Requirements" serving as rationale for screening standards for the PrivacyMark System[4], the PPC discussed on how to expand the scope of individual rights on cease of utilization, etc.

○ Regarding this point, diverse opinions were gathered by public comment procedure for the Interim Summary. Some requested mandating the cease of utilization or

[2] The PPC asks consumers and town communities or corporate officers to exchange opinions on struggles and doubts they have on the protection or handling of personal information, and holds town meeting nationwide (37 locations so far) to promote understanding toward the system for personal information protection and its operation and also to gather opinions on the system (refer to "Reference" at the end of this outline).

[3] Stipulated under the Industrial Standardization Act, the Japanese Industrial Standards (JIS) are a collection of national standards certified by the government of Japan, aiming at the improvement of products in terms of quality, performance and safety, as well as the enhancement of production efficiency and other areas.

[4] PrivacyMark System is a system set up by JIPDEC to assess private enterprises that take appropriate measures to protect personal information. Such private enterprises are granted the right to display "PrivacyMark" in the course of their business activities.

deletion while others viewed that there was sufficient room for discussions on expanding individual rights on cease of utilization. On the other hand, from the business side, some viewed that "taking voluntary measures under the current system is sufficient", "the topic needs to be carefully discussed by considering the balance between protection and utilization and referring to the EU GDPR", "exceptions need to be established", "cease of utilization and deletion need to be separately discussed", or "actual circumstances in other countries should be considered". Otherwise, some agreed to expand an individual' rights on cease of utilization etc. or to give an individual rights to control his or her own personal information.

○ Based on these opinions, in order to strengthen a principal's involvement in retained personal data while taking heed of the burden of a business operator, requirements for the cease of utilization, deletion, and cease of provision to a third party will be eased, and the scope of individual rights will be expanded in preparation for potential violations of individual rights and interests.

○ However, to alleviate the burden of a business operator, when it is difficult to cease utilization, delete, or cease providing to a third party and if alternative measures to protect a principal's rights and interests are to be taken, the business operator will be exceptionally allowed to reject these claims.

4. Enhancement of the Right of Disclosure

(1) Strengthen Efforts for Appropriate Operation

○ With regard to the right of disclosure, it was clarified as the right which can be requested in court in the 2015 Amendment Act. However, many complaints toward business operators are being received through the Inquiry Line, and in the interviews by the PPC, some business operators showed their reluctance to respond to requests for disclosure. In addition, information received through the Inquiry Line shows that some business operators do not necessarily understand the system accurately and operate the system of disclosure. In the public comments for Interim Summary, some claim that the Act is not fulfilling its purpose due to expanded interpretation of the exception provisions, and some argue that the system of disclosure needs to be easier to use.

○ Disclosure of personal information to a principal, combined with the system of notification and public disclosure of a purpose of utilization, enhances the transparency in the handling of personal information. In addition, requesting

disclosure is the premise for correction or cease of utilization, and all these combined procedures constitute a system that enables a principal's proper involvement in personal information. In this sense, the system of disclosure is one of the most important systems among the rules relating to the proper handling of personal information.

○ Based on these purposes in the Act, with regard to requests for disclosure, the PPC will continue to carefully monitor on the status of business operators' practices and continue to inform business operators of the system.

(2) Promotion of Digitalization in Disclosures

○ With regard to the form of disclosures, in the current system, Article 9 in the Cabinet Order to Enforce the APPI (Ordinance No. 507 of 2003) prescribes "method by delivering written documents" as a general rule and adds "when there is a method agreed on by a person having requested disclosure, that method".

○ However, an act that partially amends laws regarding the use of information and communications technologies in administrative procedures (so called "Digital Procedures Act") was established at the regular Diet session in 2019, in order to enhance convenience for persons involved in administrative procedures and simplification and streamlining of administrative operation by using information and communications technologies. In accordance with this act, the APPI should clarify its position on disclosures using electronic or magnetic form while taking heed of the convenience of users.

○ With regard to this point, when the PPC requested public comments for the Interim Summary, many agreed to providing information in electronic or magnetic form, but there were both opinions on whether or not to mandate it.

○ With regard to retained personal data subject to disclosure request, since it may include a vast amount of information due to the advancement of information technologies, it may be difficult for a principal whose retained personal data is disclosed by printed form to search information and sufficiently understand its content. Especially, if the retained personal data is in the form of audio or movie, it is difficult to reproduce the content in written form. As such, in some cases, disclosure through written forms do not sufficiently clarify how the retained personal data is handled, thus making it difficult to request corrections, cease of utilization, and cease of provision to a third party based on disclosure. Additionally,

when a principal uses the disclosed personal data himself or herself, electronic or magnetic form is more convenient in most cases.

○ Thus, in order to enhance the convenience of a principal in using retained personal data obtained through disclosure, the principal will be able to specify disclosure methods, including provision of electronic or magnetic record, and a personal information handling business operator (PIHBO) will be obliged to make the disclosure through the specified methods as a general rule. However, if the specified disclosure methods incur extensive costs or are difficult to take for other reasons, disclosure through delivering written documents will be allowed if a business operator notifies a principal of it.

5. Extending the Scope of Retained Personal Data to be subject to Demand for Disclosure etc.

○ With regard to retained personal data that is subject to disclosure etc., the current Act excludes those that are to be deleted within a period that is less than one year and prescribed by a cabinet order (Article 2, Paragraph 7 of the Act). The period prescribed by the cabinet order is six months, based on Article 5 of the Cabinet Order to Enforce the APPI. This is because it was considered that personal data to be deleted within a short period of time has a limited time to be handled, and has low risks of violating individual rights and interests and high probability that the information will be deleted during the period between the receipt of demand for disclosure and the actual disclosure, thereby making the disadvantages for a PIHBO in terms of costs to deal with a demand are larger than the advantages of recognizing a principal’s right to demand the disclosure.

○ However, due to the advancement of the information society, even personal data that is to be deleted within a short period of time now actually bears risks of leakage and immediate spread during the period. As such, with regard to personal data that is to be deleted within a short period of time as well, risks of violating individual rights and interests are not necessarily low. Also, if the information is already deleted, a PIHBO does not need to respond to the demands. Thus, it can be thought that the disadvantages for a PIHBO in terms of costs to deal with a demand for disclosure etc. are not necessarily larger than the advantages of recognizing a principal’s right to demand disclosure etc.[5] Furthermore, the "JIS Q 15001

[5] The PPC conducted a survey research in September 2019 to companies that are member of the Japan Business Federation, in aims to observe the actual circumstances in retention periods of personal data among PIHBOs. Results show that 42 out of 55 companies responded that there are no personal data that is to be deleted within six months. On the other hand, 10 out of 55 companies responded that "it would be problematic" if the provision on

Personal Information Protection Management System – Requirements", which serves as the basis for screening standards for the PrivacyMark system, still mandates response to demands for disclosure etc., including those for personal information that is to be deleted within six months, as a general rule, where it is observed that business operators voluntarily respond to demands at levels higher than that specified in the APPI.

○ Thus, with regard to retained personal data subject to a principal's demands for disclosure etc., they will not be limited in terms of retention periods, and the short-term data that is deleted within six months and currently excluded from the retained personal data will be considered part of the retained personal data.

6. Strengthening the Opt-Out Regulation

(1) Strengthening Enforcement

○ With regard to the so-called opt-out provisions[6], the 2015 Amendment Act introduced an obligation that a PIHBO which considers to use the opt-out system should notify to the PPC in addition to the procedures prescribed in the original APPI. The amended system is considered to be effectively functioning to a certain degree.

○ With regard to measures on list brokers, it has been raised as a problem for a long time, where the main government agency responsible for such measures was not necessarily clear. As such, the 2015 Amendment Act introduced the opt-out provisions that impose notification obligations and has enabled the PPC to deal with the issue in an integrated way. Under such circumstances, many have requested thorough execution of measures through the Inquiry Line and town meetings. Additionally, when the PPC sought public comments on the Interim Summary, many requested stringent execution of the measures on list brokers.

○ Additionally, fact-finding surveys that have been conducted by the PPC show that there are business operators who do not sufficiently fulfill the obligations of

exceptions were to be abolished, expressing concerns for increase in operations and costs. With regard to this point, even the current provisions provide exception that allow nondisclosure in "cases in which there is a possibility of interfering seriously with the business operator implementing its business properly". It can be considered that if disclosure causes significant problems for business operators to appropriately execute their operations, such provisions on exceptions should be used.

[6] A PIHBO, in regard to personal data provided to a third party, may, in cases where it is set to cease in response to a principal's request a third-party provision of personal data that can identify the principal and when it has in advance informed a principal of those matters set forth in the APPI or put them into a state where a principal can easily know, and notified them to the PPC, provide the said personal data to a third party without the principal's consent (Article 23, Paragraph 2 of the APPI).

confirmation and record-keeping or have not submitted notification yet.[7] Additionally, it has been found that there are business operators with discrepancies between the content of notifications submitted to the PPC for opt-out procedures, which help a principal to judge on opt-out, and actual operations. Furthermore, there are concerns on whether or not necessary, sufficient and specific content for a principal to decide on opt-out procedures in light of purposes of utilization of personal data after provision to a third party are being provided.

○ In light of such circumstances, the PPC has requested business operators who have submitted notifications to confirm the content of the notifications and resubmit them if necessary. Going forward, the measures on list brokers will be thoroughly taken, such as by monitoring actual operations of business operators that received guidance or the existence of business operators who operate list broker business without notification. If business operators don't handle name lists in a manner that meets the APPI, necessary measures will be taken by the PPC.

(2) Limiting the Scope of Personal Data subject to the Opt-Out Provisions

○ Furthermore, surveys conducted by the PPC have found problematic handling of information in terms of individual rights and interests such as circulating personal data, that is seemingly not obtained properly, with opt-out provisions.

○ Specifically, as far as current findings show, the majority of personal information obtained by list brokers are obtained from third parties. Some name lists handed by list brokers include those that principals do not recall providing. It can be thought that they include lists that providers extracted illegally or list brokers obtained through wrongful means. It can also be thought that some list brokers who receive the lists are aware that providers obtained them through wrongful means or can easily become aware of such fact.

○ Additionally, transactions for name lists are sometimes carried out between list brokers. In the PPC's FY 2017 research studying actual circumstances of businesses providing personal information to third parties, interviews for about 30 business operators who had made opt-out notifications discovered that close to half of the operators had transactions on personal information with other operators doing the same business.

[7] The surveys conducted in FY 2017 and FY 2018 respectively. Refer to the PPC's press release "Results of research relating to businesses providing personal information to third parties" (September 26, 2018; https://www.ppc.go.jp/files/pdf/300926_houdou.pdf) for the first and Document 2 of the 112th meeting of the PPC (https://www.ppc.go.jp/files/pdf/0726_shiryou2.pdf) for the second.

○ Furthermore, it found out that some business operators that submitted opt-out notifications (opt-out business operators), including list brokers, were not fulfilling the obligations of confirmation and record-keeping when providing or receiving personal data (Article 25 and 26 of the Act).

○ As such, in light of the fact that a principal's involvement is difficult due to the circulation of name-lists, in order to prevent an opt-out business operator from improperly obtaining personal information and to protect individual rights and interests, the scope of personal data that can be provided to a third party without the a principal's consent based on the opt-out provisions will be limited.

(3) Adding the Items subject to Notification

○ While provision to a third party based on the opt-out provisions are necessary for utilization of personal information, there are risks that personal data will be provided to a third party without a principal's consent and handled in a manner that violates individual rights and interests. The PPC needs to understand actual circumstances of such risks and exercise its authorities adequately. However, in the current Act, basic information of a business operator such as address are not legally specified as opt-out notification items, and in some cases, business operators cannot be contacted after a certain period of time has passed from the submission of notifications due to changes in addresses. In the PPC's FY 2019 fact-finding survey of opt-out business operators, when surveys were post mailed to all 158 operators as of March 31, 2019, six business operators could not be contacted since locations were unknown.

○ In order to secure proper enforcement, some basic items such as a business operator's name and address will be added as items that need to be notified. Notification of changes will be required if there are any, so that the PPC is aware of an opt-out business operator's location.

(4) Mandatory Disclosure of Confirmation and Record Duties regarding Provision to a Third Party

○ In the 2015 Amendment Act, confirmation and record-keeping regarding provision to a third party became mandatory. This obligation aims to (1) prevent personal information that is obtained through wrongful means from repeatedly circulating, and (2) secure traceability in the circulation of personal information by making duties of keeping and maintaining records mandatory. However, this "traceability

in the circulation of personal information" is from the perspective of a supervisory authority, and hence it did not secure traceability for a principal.

○ Traceability in the circulation of personal information is an indispensable factor for a principal to be able to exercise his or her right to cease of utilization or other demands. In actuality, at the PPC's Inquiry Line, the PPC receive many consultations on whether or not disclosure of sources that obtained personal information could be demanded and opinions that systems requiring disclosure of such sources should be established.

○ Thus, records when providing personal data to a third party or when receiving from a third party will be subject to demands for disclosure.

Section 2 Perspectives on Obligations that Business Operators Should Abide by

1. Mandatory Reporting of an Incident including a Leakage of Personal Data to the PPC and Notification of Such Incident to a Principal

(1) Basic Approach

○ Leakage reports are a source of information for the PPC to be informed such incidents and to protect individuals' rights and interests. It is of great significance in that proper operations by many other business operators can be promoted not only by authorities' appropriately supervising individual business operators but also by authorities' actively providing information that business operators should refer to or advice to them.

○ Reporting an incident including a leakage of personal data to the authority is mandatory in many foreign countries. On the other hand, in Japan reporting an incident including a leakage of personal data to the PPC is "an obligation to make effort" in the Japanese system, but many companies proactively report it well. It is thought that this demonstrates how awareness toward protection of personal information among Japanese business operators is penetrating.

○ Meanwhile, since a leakage report is not a legal obligation, some business operators are reluctant to report. There are concerns that if business operators did not even publicly disclose an incident including a leakage, the PPC could not take appropriate measures without learning of the event.

○ Additionally, from the perspective of a business operator, establishment of mandatory reporting of an incident including a leakage in a clear manner, with certain mitigation measures, will help the company judge whether or not the event should be reported.

○ In addition, from the perspective of trends in international discussions, it needs to be considered that multilateral frameworks such as the Global Privacy Assembly[8] and OECD are discussing on aiming to sharing each country's status on leakage reports with other authorities for efficient enforcement.

○ In the public comments for the Interim Summary, there were many opinions both for and against reporting of an incident as a legal obligation. However, it needs to

[8] Based on decisions made at the 41st International Conference of Data Protection and Privacy Commissioners（ICDPPC）held in October 2019, the name of the conference was changed to Global Privacy Assembly from November 15, 2019.

be considered that a leakage report is of great significance for a principal, a PIHBO and a supervisory authority in many ways and that it is becoming an international trend. Thus, a leakage report will be clearly specified as a legal obligation.

(2) A Incident subject to Reporting

○ Many legislation examples in foreign countries make it mandatory to report an incident including a leakage as a legal obligation, but the incidents subject to reporting obligation, deadline, mitigation measures and regulations on notification to a principal vary. In reference to such foreign legislation examples and while taking into account of effects and viability, the PPC discussed how the system should be in Japan.

○ In the public comments for the Interim Summary, there were a lot of voices that if reporting of an incident including a leakage were to be mandatory, regulations should take into consideration of feasibility for companies, and limit cases subject to reporting. Also, in addition to the fact that there were many negative opinions on setting time-related restrictions on reporting, some requested the centralization of the destination of reporting, while others mentioned that the necessity of mandatory notification to principals was not so high.

○ In making it mandatory to report an incident including a leakage, the system needs to be established in light of such opinions. There are doubts in requiring for all cases including minor ones, in terms of the burden of business operators reporting and in terms of usefulness for enforcement authorities receiving the reports.

○ In light of the above points, prompt reporting to the PPC will be mandatory in limited cases that fall under specific types, such that more than certain number of personal data is leaked or special care-required personal information is leaked.

(3) Deadline and Destination of Reporting etc.

○ While a leakage report needs to be promptly made in order for the PPC to learn of the situation and take necessary measures, time necessary for a business operator to fully understand the situation significantly depends on individual specific situations, and it is thus difficult to prescribe a fixed number of days. Thus, although clear time-related restrictions will not be established, "prompt" reporting upon limited the content to a certain level will be mandatory.

○ On the other hand, since a report on causes and measures for recurrence need to be

requested, for operational purposes, submission of a full report within a certain period of time will be requested separately from the above-mentioned prompt report.

○ On the destination of reporting, the current system allows reporting of an incident including a leakage to be submitted to not only the PPC but also delegated government agencies and accredited personal information protection organizations (APIPOs). With regard to this, in light of the fact that opinions requesting centralization of destinations of reporting were submitted at the public comment procedure for the Interim Summary and that reporting of an incident will become a legal obligation this time, submission will be limited only to the PPC or delegated government agencies.

(4) Notification to a Principal

○ By notifying a principal when an incident including a leakage of personal data happens, the principal will be able to proactively take appropriate measures, such as prevention of secondary damages or exercising of his or her necessary rights. Thus, if a PIHBO is subject to reporting specified in (2), as a general rule, it shall notify a principal.

○ On the other hand, even when an incident including a leakage of personal data happens, in fact, it is difficult to notify a principal in some cases. Specifically, it can be expected that some principals may not be able to be reached because their contacts were not included in the first place or registered contact information is old. Although notification to a principal should be made as much as possible, requiring a business operator to identify the principal's updated contacts and hence contact them, even when he or she cannot be reached based on retained information, would cause excessive burden on the business operator.

○ However, even when it is difficult to notify the principal, the PIHBO can take care of individual rights and interests and take alternative measures such as publicly disclosing and responding to inquiries. Thus, exception provisions will be established for cases when it is difficult to notify the principal but necessary alternative measures are taken to protect individual rights and interests.

2. Clarification of the Obligation for Proper Utilization of Personal Information

○ Due to the recent rapid advancement of data analytics technologies, the use of personal information that might potentially lead to the infringement of individual rights and interests has been observed, and therefore concern among consumers is

heightening.

○ Under such circumstances, especially noteworthy are some cases that are not necessarily illegal in terms of provisions in the current Act but utilize personal information in ways that cannot be overlooked in terms of protecting individual rights and interests, which is the purpose of this Act, such as using personal information in ways that may potentially facilitate or induce illegal or unjustifiable conducts.

○ In light of such circumstances, it will be clarified that a PIHBO should not utilize personal information in ways that cannot be deemed proper.

[Tentative Translation]

Section 3 Perspectives on Frameworks to Encourage Voluntary Activities of Business Operators

1. Accredited Personal Information Protection Organization System

(1) Basic Approach

○ The role of the accredited personal information protection organization system (APIPO system) was strengthened in the 2015 Amendment Act. For example, an Obligation to make efforts to develop a personal information protection guideline after listening to the opinions of multi-stakeholders was prescribed, and taking measures to make covered business operators comply with the personal information protection guideline was changed from the obligation to make efforts to the obligation.

○ The APIPO system is a unique Japanese system that aims to enhance personal information protection levels by encouraging voluntary efforts among business operators in the private sector. It is internationally drawing attention as a system that positions business operators' voluntary efforts as an important part of the Act.

○ Among APIPOs, some actively engage in efforts such as providing guidance and support to their covered business operators or specifying original rules through personal information protection guidelines. However, some engage in hardly any efforts.

○ Thus, the PPC has been driving efforts to ensure that APIPOs appropriately execute accreditation operations. Specifically, based on fact-finding surveys, the PPC encourages APIPOs that do not meet legal accreditation standards to resolve the gap and annuls accreditation of APIPOs that do not actually operate and have no prospects of resolving the disqualification.

○ Additionally, issues regarding the APIPO system is also becoming clear. For example,

- Before the 2015 Amendment Act, it was governed by respective ministers in charge, and therefore, many of the constituting organs were in industry units.
- With regard to industries in which business categories are diversifying, such as internet-related services, there are many business operators that do not necessarily join "industrial associations", and the general participation rate tends to be low.
- Although personal information protection efforts that leverage the expertise of associations that focus cross-industrially on particular businesses are desirable, APIPOs are made to focus on the overall handling of personal information by

covered business operators and cannot focus on particular businesses only under the current Act.

○ In a manner that responds to such issues, in public comments for the Interim Summary, the PPC received comments requesting accreditation in business field units instead, in order to further activate the APIPO system.

○ In light of the importance of the APIPO system and in order to enable the system to sufficiently fulfill its expected roles, the PPC has been discussing on how the PPC should provide support and on how the system should be, from perspectives of both enhancing activities by APIPOs and expanding the benefits of becoming covered business operators of APIPOs from business operators' point of view.

(2) Perspectives on Support from the PPC

○ As part of support from the PPC, the PPC holds periodic APIPO meetings where the PPC provides information and encourages APIPOs to mutually share information. Additionally, from FY 2018, as part of new efforts to expand benefits for covered business operators, the PPC holds training programs on actual business operations for the covered business operators nationwide. A total of eight programs will be held at five locations nationwide in FY2019. Furthermore, the PPC holds APIPO symposiums and strives to communicate the purpose of the APIPO system, status on activities by individual organizations, or the benefits of becoming a covered business operator. Going forward as well, further enhancement of awareness of and the level of activities by APIPOs will be strongly promoted.

(3) Diversification of the APIPO System

○ With regard to how the APIPO system should be, some believe that the precondition that a business operator may become a covered business operator of a particular APIPO as the entire company is an issue which limits the breadth of APIPO activities. With regard to large-scale companies and other companies that operate a wide range of businesses, from the companies' point of view, it may be difficult to find an APIPO that can accommodate all businesses of the entire company. Additionally, from APIPOs' point of view, they may be forced to accommodate all operations of entire companies, including even businesses that do not necessarily match their organizations’ characteristics. In actuality, at interviews conducted by the PPC, such issue was pointed out.

○ Thus, in light of the diversification of operations by PIHBOs using personal

information and changes in needs of necessary regulations, the APIPO system will be expanded so that an organization that engages in activities limited to specific businesses can be accredited as an APIPO, in addition to the current system where an APIPO should respond to complaints regarding the overall handling of personal information by its covered business operators and provide guidance to them.

2. Promotion of Voluntary Efforts by the Private Sector

(1) Basic Approach

○ A system design that respects voluntary efforts by business operators in the private sector have been woven into the APPI, including the APIPO system.

○ Especially in new areas that utilize digital technologies, problems associated with personal information protection are easy to occur. Since business models and technologies in such areas rapidly change, it is preferable that the private sector drives the devising of voluntary rules in a manner to complement legal regulations, and it is necessary to further promote such efforts.

○ Specifically, it is thought that efforts such as Privacy Impact Assessment (PIA), designation of a person responsible for the handling of personal data, and systems that recommend companies' voluntary efforts are to be promoted.

(2) Recommendation of PIA

○ With regard to PIA, it is an effective method for business operators, especially for those who handle huge amount of personal data, to drive necessary and sufficient efforts in an efficient and effective manner including management of personal data and effects of education to employees by assessing in advance based on this process.

○ In the public comments for the Interim Summary, there were opinions that PIA should be used as mitigation measures at times of leakages of personal information and that PIA should be considered as an obligation to make efforts and, in certain cases, should be considered as an obligation.

○ On the other hand, since the number of business operators that voluntarily perform PIA based on their own standards is increasing, and one of the international standards (ISO/IEC 29134: 2017) is being incorporated into Japan Industrial Standards (JIS), there are concerns as of this point that mandating PIA by prescribing assessment criteria and methods may inhibit such voluntary efforts. It is preferable to encourage voluntary efforts among the private sector in light of such

trends.

○ In order to encourage voluntary efforts among the private sector, the PPC will discuss measures going forward, such as compiling use cases of PIA or establishing an award.

(3) Recommendation on Establishing a Person Responsible for Handling of Personal Data

○ With regard to establishing a person responsible for handling of personal data, it is effective to enable such person to provide guidance and supervise divisions and employees on the handling of personal information in a cross-divisional manner and from an expert standpoint, as a part of establishment of system for the protection of personal information.

○ Partially mandating the establishment of such person may be considered as an option, but in light of the fact that a certain number of companies have been voluntarily establishing divisions in charge of making advice to company-wide handling of personal information, prescribing requirements and operations and hence mandating them to all may inhibit such voluntary efforts.[9] Thus, alike PIA, encouraging voluntary efforts is preferable.

(4) Enriching the Contents of Public Disclosure regarding Retained Personal Data

○ With regard to establishing structures to protect personal information and the contents of efforts to ensure proper handling, voluntary action of business operators in accordance with the nature of the information they handle is expected. In order to promote such efforts, it is important that some type of framework is established to enhance awareness levels of business operators and their management.

○ Thus, in order to enable a principal's appropriate understanding and involvement and to promote proper handling by a PIHBO by enhancing the PIHBO's explanations to the principal on retained personal data, items that should be explained to the principal including structures in handling personal information, the content of measures taken, and how retained personal data is processed will be added as legally required public disclosure items (may be prescribed in the Cabinet Order).

[9] According to a survey study on business operators, business operators that have divisions in charge of supervising company-wide personal information protection constitute 68.5% of all operators, and those among large-scale operators are at 86.0% ("Study on actual circumstances of efforts by business operators for personal information protection", PPC Secretariat, March 2018).

[Tentative Translation]

Section 4 Perspectives on Policies for Data Utilization

1. Anonymously Processed Information System

○ It is recognized that a certain number of companies have already used anonymously processed information system. However, in surveys to companies, some responded "We do not know how to use it", "We do not know if there are any such needs for our company's data", "We do not have personnel who can analyze it", or "Reputational risk is a problem". It is thought that a big factor behind such feedback is that companies do not necessarily understand specific utilization models for anonymously processed information.

○ Regarding this point, in the public comments, many requested to have best practices shared, and some requested that environments where business operators can easily utilize the system to be developed. Thus, it is important for the PPC to share specific utilization models and best practices.

2. Introducing "Pseudonymised Information (tentative name)"

○ It is acknowledged that some business operators use a method that is called "Pseudonymisation" to handle "personal data" within their organizations as a part of security control action. Pseudonymisation means replacement or deletion of description that can directly identify a specific individual, such as names, so that a specific individual cannot be identified from the data itself.

○ As such business practice is widely conducted and information technology advances, by pseudonymising personal information, PIHBOs can secure a certain level of safety and maintain utility of data at the same levels as before the processing, enabling more detailed analyses than with anonymously processed information by a relatively easy processing method. Thus needs of Pseudonymised Information is increasing.

○ In the EU, based on the premise that pseudonymised information must be handled as personal information, "Pseudonymisation" is prescribed where part of the rules for personal data would not be applied as exception in certain cases, and the use of the pseudonymisation is internationally spreading. In Japan, there have been requests from the business sector for provisions on intermediate forms of information between personal information and anonymously processed information, such as pseudonymised information. In the public comments for the Interim Summary, many supported the introduction of "Pseudonymisation" with a premise of clarifying the relation with already-existing anonymously processed information.

○ Especially, with regard to pseudonymised personal information, if conditions are set to prohibit the restoring of the personal information used for the production and the identification of a specific individual, it will not be used in linkage to a principal, and the risks of violating individual rights and interests will be reduced to a significant degree. Meanwhile, analyzing and using such information within companies is important in terms of enhancing competitiveness of Japanese companies.

○ Thus, from the perspective of securing safety and promoting innovation, "Pseudonymised Information (tentative name)" will be introduced, as a category of personal information that is processed so as not to be able to identify a specific individual unless it is collated with other information. With regard to "Pseudonymised Information (tentative name)", based on the premise of certain conduct regulations to limit the utilization to business operators' internal analyses without identifying a principal as well as specification of a utilization purpose of "Pseudonymised Information (tentative name)" and its disclosure to the public, obligations of dealing with demands from individuals (demand for disclosure, correction, cease of utilization, etc.) will be eased and "Pseudonymised Information (tentative name)" will be made available for various analyses.

○ In general, it is assumed that a business operator who produced "Pseudonymised Information (tentative name)" retain original data used to produce. Thus, although a principal cannot make various demands for "Pseudonymised Information (tentative name)", which a specific individual cannot be identified by itself, the principal can make such demands for the original data (retained personal data).

○ Considering "Pseudonymised Information (tentative name)" is used for the internal analyses within a business operator, "Pseudonymised Information (tentative name)" itself will not be allowed to be provided for a third party. However, it is permitted for a business operator to provide the original data used to produce the "Pseudonymised Information" with the third party when the business operator obtains a principal’s consent[10].

3. Clarification of Exception Provisions regarding the Handling of Personal Information

[10] By obtaining principal’s prior consent, etc., it is allowed to provide pseudonymised original data, in addition to the original data, as personal data to the third parties.

for Public Interest Purposes

○ The collection and analysis of big data, including customer information, is becoming possible due to the rapid advancement of information communications technologies. Such analysis results are starting to be used to resolve social issues, for example in areas such as revitalization of local communities or healthcare and nursing care.

○ Under such circumstances, further use of data is being sought for in Japan, such as implementing advanced technology for big data analysis in various industries and social life to materialize Society 5.0, a new society where both economic growth and resolution of social issues are achieved. As social issues diversify, in order to resolve such issues efficiently and effectively, it is desirable that the development of environments where business operators can utilize data is supported.

○ With regard to this point, the current APPI specifies exception provisions on purpose of use and restrictions on provision to a third party, such as "cases in which there is a need to protect a human life, body or fortune, and when it is difficult to obtain a principal’s consent" or "cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal’s consent", which means that it is considered that it allows use of personal information for public interests in certain circumstances. Since such exception provisions tend to be interpreted in a strict manner, these interpretations will be clarified by guidelines and Q&As according to assumed demands, and thus the use of personal information which brings benefits such as resolution of social issues to Japanese citizens in general will be promoted.

○ Some cases that may be specifically clarified are, for example, medical institutions and pharmaceutical companies use personal information to advance medical research, aimed at achieving healthcare services, pharmaceutical products, and medical devices that are in high quality in terms of safety and effectiveness.

4. Handling of Device Identifiers

(1) Basic Approach

○ In Internet business, information on such as users' registration, action history, and used devices to browse (user data; may include personal information and user information other than personal information) are increasingly being obtained and used.

○ A typical example is the Internet advertisement business. When users access a particular website, user data regarding each user's interests, preferences, gender, age, and area of residence are obtained through cookies of each browser in the user's PCs or smartphones. So-called targeting advertisement, which distributes advertisement to users targeted based on such user data, is spreading widely.

○ Such business models using device identifiers are very complex and diverse. Internet technologies, which are the foundation of targeting advertisement, are significantly advancing, and in order to avoid inhibiting innovation, it is important that they are first appropriately operated based on voluntary rules. On the other hand, while making full use of voluntary efforts by the private sector, ways of effective enforcement such as utilizing the APIPO system need to be discussed.

○ Furthermore, with regard to improper handling of user data in terms of individual rights and interests that cannot be overlooked, appropriate measures need to be taken by the PPC and the system needs to be verified.

(2) Proper Handling of Device Identifiers

○ Even if they are device identifiers, if a specific individual can be identified when linked to such as member information, the information must be handled as personal information as specified in the APPI. However, there are cases where some business operators demonstrate a seemingly lack of understanding, thus the actual practices need to be carefully monitored and appropriate communication and measures are required.

(3) Handling of Information that is Personal Data for a Recipient

○ Although targeting advertisement sometimes use personal information, they often use only user data that does not include personal information. Even if the information is user data linked to identifiers such as cookies, the information will be considered as personal information if it can be readily collated with other information and thereby identified a specific individual. However, it has been customary in the advertisement industry to handle the targeting advertisements in a manner that does not identify an individual in many cases.

○ Meanwhile, in recent years, the use of platforms called data management platforms (DMP) which collect, accumulate, integrate and analyze online user data has become popular[11]. Under such circumstances, businesses that provide other

[11] Among DMPs, "private DMPs" are used by companies to utilize data that they themselves accumulate, while

business operators with non-personal information user data linked to identifiers such as cookies, while being aware in advance that the information would become personal information as the recipient collates them with other information, are emerging.

○ Due to the advancement and penetration of technologies that collect vast amounts of user data, swiftly collates them, and turns them into personal data, schemes that provide non-personal information to a third party, despite being aware that the information will be turned into personal data at the recipient’s side, thereby circumventing provisions in Article 23 of APPI, are spreading. There are concerns that such collection of personal information in which a principal is not involved will spread.

○ The APPI regulates information regarding a living individual that can identify a specific individual as personal information. This includes information that can identify a specific individual by itself and also information that can identify a specific individual if a business operator readily collates it with other information internally.

○ The APPI requires a PIHBO to appropriately handle personal information. Thus, when providing the information to an external party, even if the information itself is not personal information, the APPI requires the provider to properly provide the information as personal information if "the information can be readily collated with other information and hence enable identification of a specific individual" at the provider’s side.

○ The basic principle is that a business operator that retains personal information is to bear primary responsibility for individual rights and interests, and thus a provider is required to handle such information as personal information, even if the information cannot be recognized as personal information on the recipient’s side (generally called "Provider Standards").

○ However, with regard to a recent issue where information "does not fall under personal data on the provider’s side but does so on the recipient’s side", legal interpretation is not clarified.

"public DMPs" are used by business operators that collect user data from various other business operators, allocate IDs, integrate, and analyze the information, and hence provide them to external parties.

○ Thus, while maintaining the above Provider Standards as the basic rule, regulations that restrict provision of personal data to a third party will be applied to information which does not fall under personal data on the provider’s side but clearly becomes personal data on the recipient’s side.

5. Enhancement of Consultations on Utilization of Personal Information taking into account Its Protection and Utility.

○ With regard to the handling of personal information including its utilization, the PPC have received opinions from PIHBOs, through interviews as well, requesting the development of environments where they can easily consult with the PPC.

○ Although the PPC has accepted individual consultations from industrial associations and business operators as necessary, its consultation support will be enhanced and strengthened in order to appropriately respond to voices mentioned above. Specifically, the PPC will newly establish the "Support Desk for Effective Utilization of Personal Data" (tentative name). It will actively accept consultations on especially topics related to new business models or common concerns in an industrial association or multiple business operators, and support the consultees in properly and effectively using personal data.

○ Additionally, the PPC will share knowledge on generalized best practices gained through consultation support, paying attention to protect know-hows of businesses, to the general public in an appropriate manner on the PPC's website, and will share information that is considered widely beneficial through guidelines and Q&As. Through such measures, environments where business operators can better consider the utilization of personal data will be developed.

6. Necessity of International Efforts for Data Utilization.

○ It is important that appropriate measures for protecting personal data are taken when promoting global data utilization. The PPC have globally discussed privacy issues in 2019. As part of that, the PPC held (1) the Asia Pacific Privacy Authorities (APPA) forum to seek opportunities for cooperation on enforcement activities across the Asia Pacific region, and (2) the International Seminar on Personal Data as a G20 side event, aiming at further awareness of the importance of developing a framework for data free flow with trust while protecting personal data and of relevant issues.

○ Leveraging the relationship with the EU that were built through developing the

framework for smooth personal data flow (so called "Mutual Adequacy Recognition") and the relationship with the U.S. that were built through promoting Cross Border Privacy Rules (CBPR) of the Asia Pacific Economic Cooperation (APEC), it is important that the PPC continues to lead international discussions on the protection and utilization of personal data.

○ Additionally, with regard to the relationship between AI and protection of personal data or privacy, discussions have already started at the Global Privacy Assembly. Discussions on AI are underway among relevant government agencies in Japan as well. From the perspective of international cooperation, active contribution to discussions on AI and data protection will be continued, taking into consideration the status on relevant domestic discussions.

Section 5 Perspectives on Penalties

○ The APPI has the system to impose penalties on PIHBOs that are of not more than one year of imprisonment or not more than 500,000 yen of fine. There are discussions pointing out that such penalties are insufficient to control illegal conduct and need to be reinforced.

○ In light of international trends after the enforcement of the 2015 Amendment Act, it cannot be denied that reinforcement of penalties is a major trend. However, from the viewpoint of an international comparison, national legal structures and approaches to penalties differ depending on countries. Therefore, the PPC has been discussing what is preferable for Japan, taking into consideration the country's actual circumstances and legal structures.

○ Currently, with regard to violations in handling of personal information that the PPC identified, the misconducts have been redressed through providing guidance etc. This is surmised that this is due to the fact that the cost of losing consumers' trust is significant for companies. In fact, in interviews we heard from the business sector that business operators comply with the APPI and careful consideration is required for reinforcing penalties.

○ However, the number of leakage reports submitted to the PPC and requiring reports or onsite inspections have been increasing. Although there had been no cases of recommendations, orders and penalties when the Interim Summary was published, the PPC issued a recommendation for the first time in August 2019. In this case, the subject had not taken appropriate security control action nor obtained necessary consent from principals when providing personal data to third parties. Considering the severity of the case, the PPC issued a recommendation to take necessary measures, such as reviewing of organizational structures and changing mindsets to begin with, so that individual rights and interests are properly protected. In light of such serious violations occurring, the necessity to protect individual rights and interests is increasing.

○ The APPI has a system of penalties as a last resort to secure efficacy in cases of violation, and includes so-called dual penalties for legal entities (Article 87 of the APPI). The effect of the financial penalty is largely dependent on the solvency of the subject charged. Since some PIHBOs have sufficient solvency, even if financial penalty imposed on the actor is equally imposed on the legal entity under current Act, it cannot be expected to have sufficient deterrence effect as a penalty.

○ Therefore, revision on the current statutory penalties will be made as necessary, including introduction of a system to impose severer punishments on legal entities.

Section 6 Perspectives on Extraterritorial Application of the APPI and Perspectives on Efforts for International System Harmonization and Cross-Border Transfer

1. Basic Approach

○ Japan is striving for global coordination, for example by driving efforts such as Mutual Adequacy Recognition with the EU and APEC's CBPR system. Reflecting the fact that international data flow will increase hereafter, international harmonization among systems will increasingly be important. In the personal information / privacy area, as worldwide countries including developing countries engage in personal information protection legislation, state-led digital protectionism is emerging in some countries. Under such circumstances, the PPC needs to continue leading international discussions with countries and organizations, especially with the U.S. and the EU with whom the PPC has been building positive relationships, review international guidelines regarding personal information protection, seek international harmonization among systems based on those, and in compliance with such efforts, securing personal data protection and smooth flow in an appropriate manner.

○ Bilateral and multilateral international discussions regarding such personal information systems are becoming active in the past several years. In the 2015 Amendment Act, the provision "(the government) shall take necessary action in collaboration with the governments in other countries to construct an internationally conformable system concerning personal information through fostering cooperation with an international organization and other international framework." was added as Article 6 of the APPI. Based on this provision and developments in recent international discussions, in order for Japan to lead such discussions and make efforts to harmonize international systems, international negotiations function of the PPC needs to be strengthened.

2. Expansion of Scope of Extraterritorial Application

○ With regard to the so-called extraterritorial application, the scope of application of the Act was clarified in the 2015 Amendment Act. As a result, the Act is applied to a PIHBO in a foreign country that handles personal information or anonymously processed information produced by using the personal information when (1) the PIHBO supplies a good or service to a person in Japan and (2) the PIHBO acquires personal information of the person (Article 75 of the APPI).

○ However, under the current Act, provisions regarding reporting, onsite inspections and orders are not applied to a foreign business operator. The authority that the PPC

can exercise to a foreign business operator subject to extraterritorial application is limited to those that have no enforcement power, such are the provision of guidance, advising or recommendation, and excludes the collection of reports, onsite inspections and orders.

○ So far, improper handling by a foreign business operator has been corrected by guidance through the outlet located in Japan. However, when conducts that violate obligations by a foreign business operator are found and if stronger measures are necessary, for example when no improvements can be seen after providing guidance, advice or recommendations, the PPC is to request a foreign authority that enforces a foreign law equivalent to the APPI to cooperate in taking measures based on the foreign law (Article 78 of the APPI), based on the principle of reciprocity, and thus secure efficacy.

○ However, in the public comments for the Interim Summary, while some opposed the expansion of extraterritorial application, others supported the strengthening of measures for foreign business operators.

○ Additionally, there were 10 leakage reports and four cases of guidance or advice on foreign business operators in FY 2017, while there were 20 leakage reports and 15 cases of guidance or advice in FY 2018. As such the number of cases is increasing. Taking this trend into consideration, some point out that the situation is problematic in terms of fairness between domestic business operators and foreign business operators.

○ Based on such circumstances, a foreign business operator that handles personal information or anonymously processed information of an individual in Japan will be subject to collection of a report and an order, which are enforced with a penalty. Additionally, if the business operator does not abide by the order, the PPC may publicize the fact. Furthermore, onsite inspection of a foreign business operator by the PPC will be allowed. Since public authority cannot be exercised in territories of other countries without the countries' consent, due to the sovereignty of foreign countries, cooperation with foreign authorities will be made as necessary.

○ In addition, in order to effectively exercise authority and secure appropriate procedures with domestic and foreign business operators, procedures regarding service by the consul and service by publication will be specified.

3. Reinforcement of Restrictions of Provision of Personal Data to a Foreign Third Party

○ As foreign outsourcing increases and business models become complex, risks that are associated with cross-border transfer of personal data are changing. So far, data protection-related laws complied with OECD Privacy Guidelines in many countries. However, as data protection-related laws are spreading worldwide including developing countries, state-led digital protectionism is emerging in some countries. Data localization which mandates domestic retention of data and legislations regarding unlimited government access to private sector data are examples of state-led digital protectionism.

○ As cross-border transfers of personal information increases, such differences in systems among countries and regions make predictability for business operators that handle personal data unstable and raise concerns in terms of protection of individual rights and interests. For example, in association with data localization policies, there are concerns that a foreign business operator that receives cross-border transferred information will not be able to attend to a principal's demands for deletion of personal data or that personal data obtained in and cross-border transferred from Japan may be improperly used due to unlimited government access by a foreign government. Such state control regulations may incur risks that cannot be overlooked in terms of protection of individual rights and interests.

○ Additionally, at the G20 Ministerial Meeting on Trade and Digital Economy in Tsukuba, Ibaraki in Japan (held on June 8 and 9, 2019), the G20 members unanimously consented upon the concept of "Data Free Flow with Trust", and trustable legal frameworks of respective countries must be mutually accessible. Under such international trends, in order to achieve "promotion of free data flow internationally, which facilitate unfettered flow of data, that is beneficial to resolving business and social issues without national border concerns, while ensuring reliability related to privacy, security, and intellectual property rights", in addition to that mutually trustable free flow of data needs to be promoted among countries, it is important that trust, which supports the free flow of personal data as in the above, needs to be secured between business operators and principals as well.[12]

○ Article 24 of the APPI, which was introduced in the 2015 Amendment Act, restricts a PIHBO's foreign transfer of personal data in certain cases and applies to a sending domestic business operator in foreign transfer. In order to respond to risks that arise

[12] Follow-up on the Growth Strategy (decided at June 21, 2019 Cabinet Meeting)

from the diversity of situations at the destination, minimal attention to a recipient business operator and a country where the recipient is located needs to be paid.

○ Specifically, when transferring personal data based on a principal's consent, a sending PIHBO will be required to enrich the information provided to the principal regarding the handling of personal information at a recipient business operator, including the name of country and whether or not the country has systems for personal information protection. Additionally, when transferring personal data without a principal's consent, under the condition that a system is established to ensure continued proper handling of personal data at a recipient business operator, in accordance to the request by the principal, a sending business operator is to provide information regarding the handling of personal data by the recipient business operator.

○ With regard to the providing information to a principal on the system of personal information protection at a destination country, the extent is to be at a minimal degree and does not have to be comprehensive since the purpose of the provision is to enhance predictability for the principal on how the personal information will be handled. Hereafter, the content of information to be provided and the method of provision will be specifically discussed, while sufficiently taking heed of the burden on business operators and their operations to avoid overburden.

[Tentative Translation]

Section 7 Handling of Personal Information by Public and Private Sectors

1. Basic Approach

○ In the public comments for the Interim Summary, there were many opinions that requested the integration of laws for administrative organs, incorporated administrative agencies, local public entities and private business operators, and that requested the PPC to govern the handling of personal information by administrative organs and local public entities as well.

○ Points to be discussed concerning the handling of personal information within the public area can largely be divided into the handling of the "Act on the Protection of Personal Information Held by Administrative Organs" and the "Act on the Protection of Personal Information Held by Incorporated Administrative Agencies", and the handling of ordinances of personal information protection for local public entities.

○ With regard to the handling of personal information in the public area, demand to secure reliability in protecting collected personal information is high since administrative organs can collect personal information by exercising public authority. On the other hand, as for the private sector, attention needs to be paid to enable freedom of business. Thus, it is regarded that a certain degree of difference in the way personal information is handled needs to be allowed. Meanwhile, with regard to the handling of personal information amongst public and private sectors, it is required that systems that match and are in harmony with both public and private sectors need to be discussed and operated, upon contemplating how the overall legislations of personal information protection should be.

○ The PPC which governs the APPI, the basic law for public and private sectors, develops the Basic Policy on the Protection of Personal Information and supervises the handling of personal information in the private sector will need to proactively proceed with discussions while gaining the cooperation of relevant government agencies and others.

2. Consolidation of Legal Systems relating to Administrative Organs and Incorporated Administrative Agencies and Legal Systems relating to the Private Sector

○ With regard to personal information protection systems relating to administrative organs and incorporated administrative agencies, the PPC will proactively and swiftly engage under the concrete discussion as the government in gathering and consolidating regulations regarding personal information protection relating to the

private sector, administrative organs, and incorporated administrative agencies and toward having the PPC centrally govern the consolidated systems, based on the indication that troubles are arising due to the differences in regulations and jurisdictions.

3. Personal Information Protection System of Local Public Entities

○ The handling of personal information by local public entities are prescribed by ordinances. Since there are many personal information protection ordinances that had been established earlier than the APPI was enacted, the actual circumstances differ according to the local public entities. With regard to this point, it cannot be said that sufficient discussions have been made on how the personal information protection systems of local public entities should be in the mid to long-term. Thus, as an opportunity to exchange practical opinions among relevant parties, the establishment of a "Meeting Regarding the Personal Information Protection System of Local Public Entities", consisted of the PPC, local public entities etc., was decided in October 2019 and has been held since December 2019.

○ Hereafter, with regard to the handling of the local public entities' personal information which is currently prescribed by ordinances, it will be discussed with local public entities etc., regarding handling of personal information held by local public entities, which is regulated by each local ordinance, on practical issues regarding the perspective of integrating the regulations by law as well as the allocation of roles between central and local bodies concerning personal information protection of local public entities.

[Tentative Translation]

Section 8 Issue under Continuous Consideration

(Surcharge System)

○ With regard to the introduction of surcharge system, while there are opinions requesting it as part of measures to strengthen penalties, many from the business sector opposed the idea in the public comments for the Interim Summary.

○ The surcharge system aims to deter violations in advance by imposing financial disadvantages to business operators that violate regulations. The current Act plans for only criminal penalties as methods to secure final efficacy. The surcharge system supplements the limitations in criminal penalties and contributes to securing efficacy of regulations.

○ Furthermore, it is necessary to execute the Act on foreign business operators that violate regulations, subject to extraterritorial applications, in the same manner as on domestic business operators. The surcharge system may be an effective means to secure execution against foreign business operators.

○ Additionally, among personal information protection legal systems in foreign countries, there are examples of securing efficacy of regulations by imposing high amount of financial sanctions on violators.

○ On the other hand, in many of surcharge system examples in other Japanese laws, surcharges are calculated based on fraudulent gains. There are inherent restrictions in the Japanese legal system, and such legal challenges need to be solved to introduce surcharge system in the APPI.

○ With regard to the introduction of surcharge system, discussions will be continued taking into consideration the Japanese legal structures, results and effect of execution, actual circumstances of domestic and foreign business operators, and international trends.

[Reference]

In preparing this outline, opinions gathered through the following activities were referred to.

1. Opinions gathered through the Inquiry Line for APPI

From May 30, 2017, the desk prepared in the PPC secretariat* receives inquiries, complaints, and mediation regarding the handling of personal information (about 75 cases per day on average, between May 30, 2017 to September 30, 2019). Opinions gathered here have been analyzed and referred to.

*A service that was reorganized from the former "Question Hotline for APPI", at the time of full enforcement of the amended APPI (May 30, 2017).

2. Opinions submitted in the Public Comment Procedure for the Interim Summary

It was conducted during the period from April 25, 2019 to May 27, 2019, and a total of 525 opinions were received from 137 organizations, business operators, and individuals. The breakdown of the number of those who submitted opinions and the content of opinions were as follows.

○ Those who submitted opinions: Total 137
- Various organizations/business operators: 54
- Individuals (including those anonymous): 83

○ Number of submitted opinions: 525
- Most received topics were cessation of utilization (65 cases), opt-out and list brokers (43 cases), leakage reports (35 cases), and targeting advertisement (36 cases).

3. Town Meeting

In order to have consumers, residents' associations, and corporate parties who are related to personal information on a daily basis exchange opinions regarding struggles and questions on protection and handling of personal information, further their understanding toward personal information protection systems and their operation, and share opinions regarding the systems, town meeting are held nationwide (at 37 locations nationwide so far).

Venue	Date	Participants
Oita Prefecture	June 11, 2018	2 consumers, 1 consumer affairs consultant, 1 member from a residents' association, 1 member from a company

Shiga Prefecture	December 18, 2018	2 members from consumer groups, 1 consultant affairs consultant, 1 member from a residents' association, 1 member from a company
Aomori Prefecture	January 22, 2019	1 consumer, 1 consultant affairs consultant, 1 member from a residents' association, 1 member from a company
Shimane Prefecture	January 30, 2019	1 PTA member, 1 consultant affairs consultant, 1 member from a residents' association, 1 member from a company
Aichi Prefecture	February 5, 2019	2 consumers, 1 consultant affairs consultant, 1 member from a residents' association, 1 member from a company
Kochi Prefecture	February 12, 2019	2 consumers, 2 member from a residents' association, 2 members from a company
Tochigi Prefecture	February 22, 2019	1 consumer, 1 consultant affairs consultant, 1 member from a company
Ehime Prefecture	July 12, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company
Fukuoka Prefecture	August 5, 2019	1 consumer, 1 consultant affairs consultant, 1 member from a residents' association, 3 members from companies
Hiroshima Prefecture	August 30, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company
Okayama Prefecture	September 12, 2019	3 consumers, 1 consultant affairs consultant, 2 member from a residents' association, 1 member from a company
Hokkaido	September 13, 2019	2 consumers, 1 consultant affairs consultant, 2 members from residents' associations, 2 members from companies
Hyogo Prefecture	September 17, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 3 members from companies
Yamagata Prefecture	September 19, 2019	1 consumers, 1 consultant affairs consultant, 1 member from a residents' association, 2 members from companies
Niigata Prefecture	September 26, 2019	2 consumers, 1 consultant affairs consultant, 2 members from residents' associations, 2 members from companies
Tokushima Prefecture	October 2, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 1 member from a company
Kagawa Prefecture	October 3, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 1 member from a company

[Tentative Translation]

Fukui Prefecture	October 8, 2019	2 consumers, 1 consultant affairs consultant, 1 member from a residents' association, 2 members from companies
Osaka Prefecture	October 9, 2019	1 consumer, 1 consultant affairs consultant, 1 member from a residents' association, 1 member from a company
Gifu Prefecture	October 16, 2019	2 consumers, 2 consultant affairs consultants, 1 member from a residents' association, 1 member from a company
Miyagi Prefecture	October 18, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company
Tottori Prefecture	October 23, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company
Saitama Prefecture	October 24, 2019	3 consumers, 1 consultant affairs consultant, 1 member from a residents' association, 1 member from a company
Yamaguchi Prefecture	October 29, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company
Akita Prefecture	November 5, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company
Nara Prefecture	November 11, 2019	1 consumer, 1 consultant affairs consultant, 1 member from a residents' association, 1 member from a company
Toyama Prefecture	November 12, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company
Ishikawa Prefecture	November 13, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company
Kyoto Prefecture	November 18, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company
Wakayama Prefecture	November 19, 2019	1 consumer, 1 consultant affairs consultant, 1 member from a residents' association, 1 member from a company
Kagoshima Prefecture	November 21, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 1 member from a company
Yamanashi Prefecture	November 25, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company

Shizuoka Prefecture	November 26, 2019	2 consumers, 1 consultant affairs consultant, 2 members from residents' associations, 2 members from companies
Kanagawa Prefecture	November 27, 2019	2 consumers, 1 consultant affairs consultant, 2 members from residents' associations, 2 members from companies
Kumamoto Prefecture	November 28, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company
Gunma Prefecture	November 29, 2019	1 consumers, 1 consultant affairs consultant, 1 member from a residents' association, 2 members from companies
Miyazaki Prefecture	December 12, 2019	2 consumers, 2 consultant affairs consultants, 2 members from residents' associations, 2 members from company

4. APPI Symposium

On January 25, 2019, experts who engage in protection of personal information from various standpoints, such as legal activities, corporate activities, consumer hotlines, or cyber security countermeasures, were invited and an "APPI Symposium, Contemplating on personal information in daily lives from now" was held.

In the symposium, we received opinions through a panel discussion by experts from various fields, under themes such as introduction of latest trends in personal information or future of protection and use of personal information (panelists are as in the following).

Panelists
Mr. Hisamichi Okamura (Attorney-at-Law, Eichi Law Offices)
Mr. Tetsuya Sakashita (Managing Director, JIPDEC)
Mr. Ken Shimizu (Executive Officer, Seven & i Holdings Co., Ltd.)
Mr. Itsuro Nishimoto (President and Representative Director, LAC Co., Ltd)
Mr. Masaki Fukui (Manager of Consultations Department 2, Consultation Information Division, National Consumer Affairs Center of Japan)
Ms. Mari Sonoda (Secretary General, Personal Information Protection Commission Japan)
Moderator
Mr. Tsukasa Obayashi (Leader Writer, Nikkei Inc.)

5. Interview with Persons in the Business Sector and Experts, etc.

Number	Date	Name of organization
89th	February 19, 2019	The American Chamber of Commerce in Japan
89th	February 19, 2019	Information Technology Federation of Japan

92nd	March 12, 2019	The Japan Electronics and Information Technology Industries Association
96th	March 26, 2019	Japan Chamber of Commerce and Industry
96th	March 26, 2019	Central Federation of Societies of Commerce and Industry
97th	March 27, 2019	Japan Business Federation
98th	March 29, 2019	Japan Interactive Advertising Association
99th	April 1, 2019	Japan Association of New Economy
105th	May 17, 2019	Mr. Yoichiro Itakura (Attorney-at-Law, Hikari Sogoh Law Offices) Mr. Takayuki Kato (Professor, Faculty of Law, Asia University) Mr. Taro Komukai (Professor, College of Risk Management, Nihon University) Mr. Fumio Shinpo (Professor, Faculty of Policy Management, Keio University) Mr. Masatomo Suzuki (Professor, Niigata University) Mr. Hiromitsu Takagi (Senior Researcher, National Institute of Advanced Industrial Science and Technology)
106th	May 21, 2019	Ms. Kaori Ishii (Professor, Faculty of Global Informatics, Chuo University) Mr. Ichiro Satoh (Professor/ Advisor to the Director General of National Institute of Informatics) Mr. Joji Shishido (Professor, Graduate Schools for Law and Politics, The University of Tokyo) Mr. Masahiro Sogabe (Professor, School of Law, Kyoto University) Mr. Ryoji Mori (Attorney-at-Law, Eichi Law Offices) Mr. Tatsuhiko Yamamoto (Professor, Law School, Keio University) Mr. Hisamichi Okamura (Attorney-at-Law, Eichi Law Offices) (*only submitted documents)
119th	September 12, 2019	Mr. Daniel Schwartz

[Tentative Translation]

121st	October 4, 2019	Japanese Trade Union Confederation

6. Accredited Personal Information Protection Organization Symposium

On March 6, 2019, an "Accredited Personal Information Protection Organization Symposium, Contemplating the Purpose of Future Potentials of Accredited Personal Information Protection Organizations" was held.

Representatives from eights organizations participated in the two-session panel discussion and shared opinions, including requests towards the system. (Panelists are as in the following. All organizations other than the Information Technology Federation of Japan are APIPOs)

First panel discussion "Operations of Accredited Personal Information Protection Organization and Their Advantages"

Mr. Hiroshi Uchida (All Banks Personal Data Protection Council (Head of Operations, Japanese Bankers Association)

Mr. Shuhei Iida (Executive Director, All Japan Hospital Association)

Mr. Toru Manba (Managing Director, Japan Direct Marketing Association)

Mr. Kiyoshi Miyashita (Executive Director, Japan Users Association of Information Systems)

Second panel discussion "Devising and Operating Voluntary Rules"

Mr. Takamasa Kishihara (Managing Director, Mobile Content Forum)

Mr. Tetsuya Sakashita (Managing Director, JIPDEC)

Ms. Yukiko Furutani (Executive Adviser, Nippon Association of Consumer Specialists)

Mr. Shuho Nozu (Senior Expert, Accredited Subcommittee Secretariat, Information Bank Promotion Committee, Information Technology Federation of Japan)