Note: This document has been translated from Japanese original document.

# The Guidebook for Corporate Privacy Governance in the Digital Transformation (DX) Era Ver 1.3

April, 2023

Ministry of Internal Affairs and Communications

Ministry of Economy, Trade and Industry

— Change History —

| Version | Description | Responsible officer |
|---|---|---|
| 1.0<br><br>available only in Japanese | ・ Guidebook for Corporate Privacy Governance in the DX Era published. | Ministry of Internal Affairs and Communications & Ministry of Economy, Trade and Industry |
| 1.1<br><br>available only in Japanese | ・ Addition and review of examples in Section 3. The Three Requirements to Be Addressed by Business Leaders and Section 4. Key Items in Privacy Governance.<br>*Updated to upgrade examples to serve as reference, based on privacy governance activities at businesses after publication of Version 1.0.<br>・ Bibliography update | Ministry of Internal Affairs and Communications & Ministry of Economy, Trade and Industry |
| 1.2<br><br>available only in Japanese | ・ Addition of examples in Section 3. The Three Requirements to Be Addressed by Business Leaders, Section 4. Key Items in Privacy Governance and Section 5. Reference: Approach to Privacy Risk Treatment.<br>*Updated to upgrade examples to serve as a reference, based on privacy governance activities at businesses after publication of Version 1.1.<br>・ Review of existing descriptions in relation to the amendment of the Act on the Protection of Personal Information, etc.<br>・ Bibliography update | Ministry of Internal Affairs and Communications & Ministry of Economy, Trade and Industry |
| 1.3 | ・ Organization of the concepts.<br>・ Addition of Section 6. Reference: Information Collection Methods in Relation to Foreign Laws and Regulations, etc.<br>・ Bibliography update | Ministry of Internal Affairs and Communications & Ministry of Economy, Trade and Industry |

TABLE OF CONTENTS

# 1. Position of this Guidebook

To realize Society 5.0, a human-centered society that highly integrates cyber space (virtual space) and physical space (real space), business enterprises play a central role in fostering economic growth and resolving social issues by creating innovations through data utilization and greater sophistication of products and services.

In the field of personal data[1] utilization, expectations expanded toward the resolution of social issues through innovation. However, there is a growing demand for careful attention to privacy. In response to this demand, business enterprises must gain an understanding of consumer consciousness and anxieties toward personal data utilization, as well as the information, actions, etc., that consumers require. They also must assess the actual status of this area to demonstrate consistency in protecting consumer privacy and hence win consumer trust and advantages in their corporate business operations. This Guidebook compiles information on how business enterprises taking on new challenges should actively work to resolve privacy-related issues and build privacy governance that leads to building consumer trust, which is essential in facilitating business execution.

This Guidebook has been compiled specifically for business enterprises that are likely to receive requests for attention to privacy directly from consumers while offering their products and services, etc., by utilizing personal data, and for vendors that conduct trade with these business enterprises.

It is assumed that it will be read chiefly by persons in the following positions in such business organizations.

- Business leaders responsible for governance in data utilization and protection, and managers in the position of submitting proposals to such business leaders, etc.
- Employees in business divisions responsible for comprehensive management of matters concerning data utilization, its application and protection, etc.

[1] Personal data refers not only to personal information under the Act on the Protection of Personal Information but also to all information relating to individuals.

Also, it is assumed that it will be used in the following situations.

- When the business enterprise has made decisions that lead to a major transition in policy direction, such as the promotion of digital transformation (DX) (i.e., in the event of changes in the business operation, business organization, process, corporate culture and/or climate, etc., by utilizing digital technology, in step with major transitions in society).
- In order to gain consumer trust and to enhance corporate value through privacy protection.
- When commencing review into a project that is assumed to have a huge impact on consumer privacy.
- When stronger action is demanded by business leaders, shareholders, investors, the parent company and other interested parties to address privacy-related issues.
- When asking business leaders for reinforcement of the organizational structure for privacy protection (i.e., when requesting appropriate allocation of management resources).
- When there are concerns such as criticism (so-called social media "flaming," etc.) that the business organization or specific industries, etc, are criticized for causing privacy-related issues in the use of personal data.[2]

The examples above are provided to promote understanding as to which situations to apply the guideline and to expand access to a broad range of interested parties.[3]

[2] Please note that this Guidebook does not cover methods on how to deal with so-called social media “flaming.”

[3] Privacy issues emerge regardless of enterprise scale or type of incorporated body. Although it may be difficult for small and medium-sized enterprises (SMEs) and venture businesses that handle personal data to do the same, such as establishment of a system for the purpose, reference to this Guidebook is recommended regarding important points of note and policies.
The enforcement of the amended Act on Protection of Personal Information in 2021 resulted in the consolidation of personal information protection laws; namely, the aforementioned Act, 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, etc., and the partial application of the obligations of private-sector business operators handling personal information to organizations other than incorporated entities, such as certain incorporated administrative agencies. Although this Guidebook has been developed chiefly with business operators in mind, the content is also useful for organizations other than businesses (including academic research institutions) and is designed to serve as a reference for a broad range of readers following amendment of the laws.

This Guidebook refers partially to legal obligations. However, each of the examples mentioned have been implemented according to the business scale and resources of the enterprise. In development of privacy governance mentioned later, the information herein should be used by adapting to the actual conditions of each business enterprise.

It must be noted that what we mean by privacy and possible impacts on privacy may change over time, as will be mentioned later. This Guidebook is expected to undergo updates in the future with attention to social trends.

In the 2020 and 2021 amendments to the Act on the Protection of Personal Information (Law No. 57; hereinafter referred to as the "APPI") that covers handling of personal information, provisions regulating the protection of personal information and privacy have been added in step with changes in the state of data utilization. At the same time, the regulations have been strengthened with descriptions in greater detail, etc.

This Guidebook specifies matters that must be addressed by business leaders to enable the entire business organization to deal with issues proactively including voluntary responses by the business and the organization to be created, along with the roles and functions it must possess, with the understanding that the matters are to be handled in compliance with the laws and regulations relating to personal information and privacy protection, not only within the statutory definition of personal information but also within the use or application of personal data that does not necessarily fall within the definition. This guidebook is expected to be used even more after the revision of the APPI.

In this Guidebook, the fundamental policy underlying compliance is set forth in Chapter 2. This is followed by Chapter 3, which describes the three requirements to be addressed by business leaders and Chapter 4, which organizes key items in privacy governance. Chapter 5 and those following present information that can be used as a reference in privacy governance.

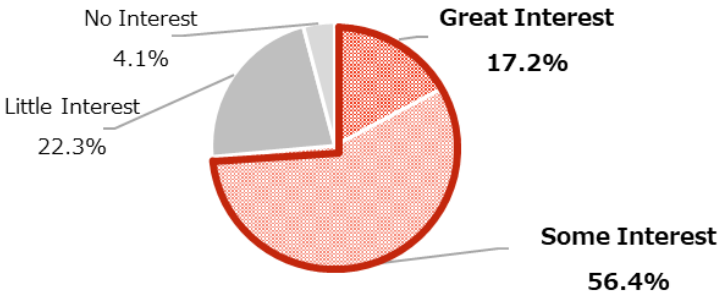
## Column: Survey on Privacy Governance

In the Survey on Privacy Governance (Overview) conducted by JIPDEC in 2021,[4] questionnaire surveys were conducted separately for consumers and businesses. The results showed that corporate efforts in the area of privacy governance have aided in the improvement of corporate value and influenced consumer behavior, proving that it has brought advantages to business enterprises.

In the responses obtained from consumers, 73.6% of consumers showed a strong interest in corporate activities related to privacy protection. Some 88.5% expressed that, in selecting among similar goods and services, privacy protection activities by the company offering goods, etc., are taken into account.

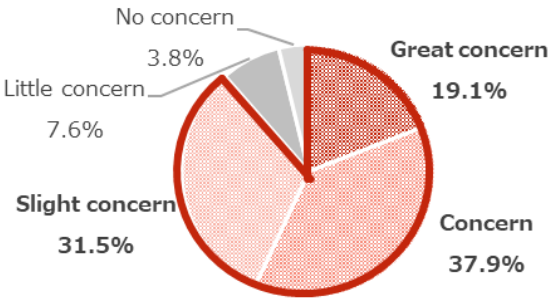
In the responses received from businesses, the results show that 58.7% believe that their activities in privacy protection will influence consumer behavior significantly.

Q: What level of interest do you have regarding privacy protection (e.g., appropriate handling of statutory personal information, data related to personal behavior and conditions not limited to statutory personal information, highly private information, etc.)? (Number of consumers: 314)




Total of respondents showing "great interest" or "some interest:" 73.6%

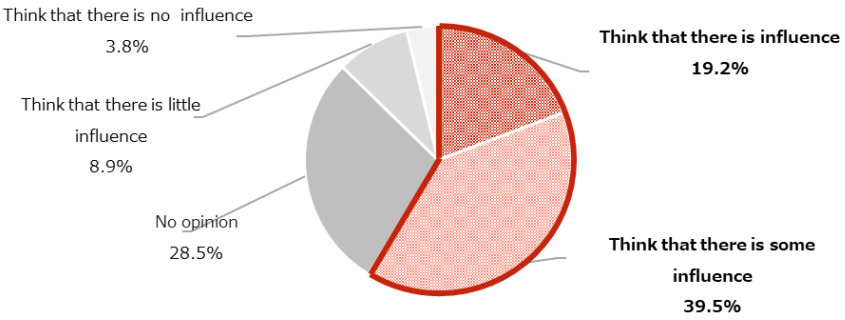
Q: If you are to choose one from among products or services that are similar in substance offered by a multiple number of vendors, what level of concern would you have regarding activities on privacy conducted by the vendors, if the product or service in question is likely to affect your privacy? (Number of consumers: 314)




Total of respondents who expressed "great concern," "concern" or "slight concern:" 88.5%

[4] "Survey on Privacy Governance (Overview) " (JIPDEC, 2021)
https://www.jipdec.or.jp/topics/news/20211018.html

Q: What level of influence do you think communicating your company's activities on privacy will have on consumer behavior? (Number of businesses: 291)




Total of respondents who "think that there is influence" and "think that there is some influence:" 58.7%

# 2. Premises of This Guidebook

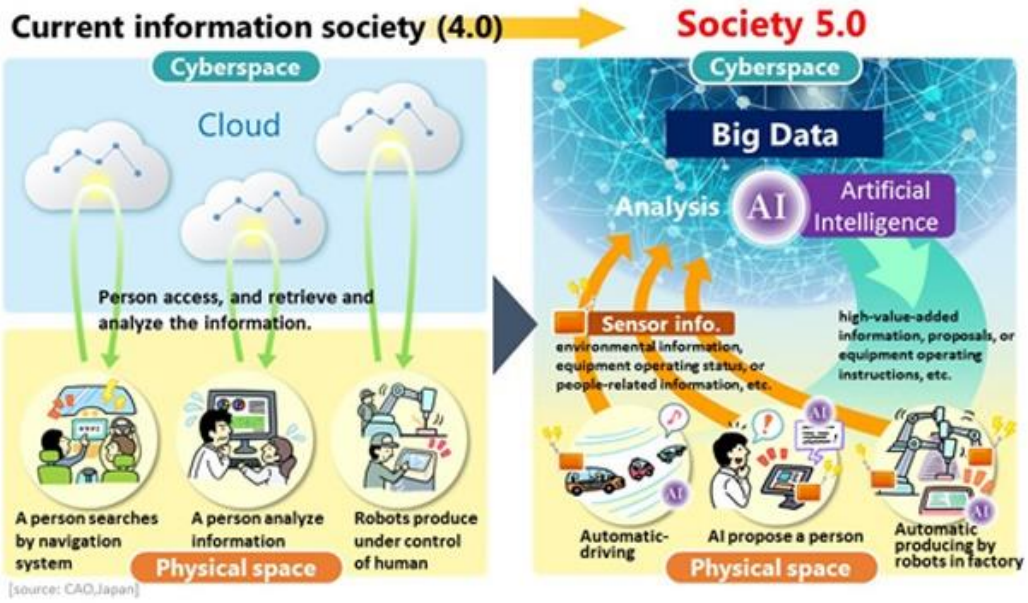
## 2.1. Society 5.0 and the Role of the Business Enterprise

Our society today is undergoing a drastic structural transition through advances in digital technology and the expansion of cyber space. Through information-collecting technologies, including highly advanced sensors and cameras, and the Internet of Things (IoT), which connects everything to the Internet, we can aggregate information about people in physical space and other objects on earth via the internet. Thus, we can consolidate the gathered information through cloud computing and other cyber space storage solutions. In addition, advances in technology, such as artificial intelligence (AI) in recent years, has enabled the estimation of various conditions in physical space. As a result, it is now possible to assess and analyze physical space as data in cyber space. The results are fed back in various forms into physical space. The Japanese government has characterized a "human-centered society that balances economic advancement with the resolution of social problems by a system that highly integrates cyber space and physical space" named as Society 5.0 and has announced this as the goal that Japan seeks to achieve.[5] To create Society 5.0, the simultaneous implementation of digital transformation (DX)[6] in both corporate management and regulatory systems is believed to be important. Furthermore, reform in digital governance is also underway in Japan's plan to build "a model realizing both innovation and social trust."

[5] Society 5.0 (https://www8.cao.go.jp/cstp/english/society5_0/index.html ), Cabinet Office

[6] Digital transformation (DX) refers to, in the case of business enterprises, the response to rapid changes in the business environment, and reforms to a company's products, services and business model in response to customer and social needs by utilizing data and digital technology. At the same time, it involves the implementation of reforms in the business operation itself, the organization, business processes, corporate culture and climate, in order to establish competitive advantage.

Figure 1. Information Society of the Past and in Society 5.0




Society 5.0, in which cyber space and physical space are highly integrated, brings innovative products, services and technology that will enrich the everyday lives of people. For example, a variety of digital platforms used on a daily basis, automated driving, which is approaching actual implementation with advances in the global race in technology development, the "smart home" that realizes comfort and security alongside conformity and sustainability with the environment, and the "smart city," which is an aggregation of those services. In such a society, functions that had been performed until now by humans or hardware in physical space will be redefined by data and software in cyber space, and will be updated frequently and evolve constantly.

With the rapid pace of change, greater ease in transnational business operation and the effects of data accumulation with indirect and direct networks,[7] innovation in cyber space is inclined to lead to “winner-take-all” results. For this reason, creative innovation, starting with the coordination of physical space and cyber space, is essential in building Society 5.0 and maintaining Japan's economic growth in the future.

[7] This refers to the effect of one person subscribing to a network and not only increasing the benefits for the person but also to other subscribers. Directly, it refers to the effect of subscriber benefit increasing with the increase in the number of subscribers of the network. Indirectly, when a certain asset is closely linked to its supplementary assets, greater use of the asset will correspondingly increase the supply of a variety of its supplementary assets, thus increasing the benefits.

Such innovation has the potential to bring solutions to social issues, including matters related to privacy. At the same time, however, new risks may emerge from such innovation. There may be situations in which such risks include new privacy-related problems. If the risks are left ignored, the innovation itself may not be accepted. For innovation to take root in society and contribute to sustainable economic growth, a social system will become necessary for society to appropriately manage the risks brought on by innovation and to establish a variety of social values, such as the safety of life, mind and body and property, privacy, democracy, and fair competition. From this viewpoint, business enterprises that are expected to play key roles in promoting innovation are to promote creative efforts actively both in terms of social value and economic value. At the same time, action must be taken to reduce the risks that emerge from this innovation. In other words, they are to conduct business while securing the trust from society and protecting the rights and interests of individual persons. Additionally, the response to social issues, including matters associated with privacy, has been previously perceived by businesses as an expense in many cases. From the viewpoint of a society that includes consumers, voluntary actions to address these issues and arrive at solutions is identical to improving the quality of the business's goods and services, etc., and is expected to improve customer satisfaction and serve as a key factor in differentiating it from its competitors. Corporate actions for privacy-related issues in the future should not be perceived as an additional cost but as inherent to the improvement of the quality of their goods and services. Business enterprises are required to shift their mindsets and work on understanding that the above is a positive sum for both business enterprises and consumers. [8]

This Guidebook focuses particularly on privacy that is closely linked to personal data utilization with this important role of businesses today in mind.

[8] An approach that covers all fair profits and goals, in contrast to the zero-sum approach that results in the creation of trade-off relationships. Refer to Chapter 7 "Reference: Privacy by Design."

## 2.2. Approach to Privacy

Advanced data utilization that is expected to become the core of Society 5.0 development differs dramatically both in quality and quantity as compared to data utilization of the past. In particular, personal data utilization enables businesses to accurately assess personal preferences and needs and is the fountainhead of business growth. Furthermore, the various activities employing a precise approach to individuals is expected to ultimately lead to the resolution of social issues and therefore are extremely important for all of society.

On the other hand, progress in personal data utilization is deeply linked to the diversification of the impacts on personal privacy.

In the data-collecting phase, for instance, the provider of a digital service will be able to assess in detail each person's behavior history, state of health, religion or creed, personal interests, and hobbies, etc., through massive and detailed collection of personal data. In this way, it is highly likely to have an impact on personal privacy. There are possibilities that the foundations of democracy might be threatened, for example, in politically targeted advertising by use of personal data.

In the data-analysis phase, algorithm-based decision-making without human intervention, including AI based on machine learning, may present growing problems in terms of security and appropriateness as the technology assumes a larger role in society. In machine learning, for example, estimation and decision-making about the target are executed through a model based on statistically processed existing data. It is therefore difficult to deal with new targets and changes in conditions, thus eroding its accuracy in estimation and decision-making. For this reason, errors are likely to occur in estimation or decision-making about the ever-changing and fluctuating physical space. It may result in errors in the target or its characteristics. If erroneous estimation or decisions in cyber space are fed back into physical space, the error may escalate discrimination or prejudice against individuals or raise risks that lead to accidents. Additionally, it is also known that erroneous estimation or decision-making is likely to occur when there is bias on the data for existing conditions that serve as the model for machine learning, as well as when statistical processing is inappropriate.

**Figure 2　Reference: IoT and AI Utilization and Privacy-Related Issues (Examples)**

| | |
|---|---|
| Use of IoT appliances, etc. | When data is obtained from consumers via IoT appliances, etc., the consumer cannot easily recognize that data is being collected. Even when it can be recognized, problem related to the fact that there is no opportunity to reflect the consumer's intention regarding the data acquisition are likely to occur. In addition, caution is required regarding data acquired by IoT appliances, etc., since the data may involve persons other than the target consumer (such as captured images by a camera).<br>・ Data to be measured (What): Difficult to determine what data is measured by the IoT appliance.<br>・ Location and time of measurement (Where and When): Difficult to determine when and where the measurement is made.<br>・ Interpretation of measured data (How): Difficult to determine how the measured data will be interpreted.<br>・ Measuring entity (Who): Difficult to determine who is obtaining data.<br>・ Purpose of measurement (Why): Difficult to communicate to the customer the purpose of measurement utilization. |
| Inference to Identify a Specific Person Utilizing AI | In terms of data use, when data obtained directly from the consumer is limited, inference and machine decision-making on attributes, etc., concerning a person based on the person's behavior, etc., employing AI, etc., (including so-called profiling) are likely to cause inference or decision-making errors and furthermore cause problems associated with privacy[9]. |

Previously, privacy has been regarded as "the right or legal protection against reckless disclosure of private lives" or "the right to be left alone."[10] In light of advances in information and communication technologies and the rise of the concept of data privacy, the concept of privacy has evolved into the concept of "control of self-information," etc., in cooperation with the expansion of the belief that respect for the rights of the individual is necessary. With technological innovations represented by IoT and AI in recent years and the rapid pace of change in services utilizing such technologies, new problems associated with privacy have appeared; namely, unfair and discriminatory treatment implemented mechanically as a result of data analysis and the possibility of intervention in a large number of voters regarding their political choice.[11]

[9] Other reference materials include "OECD Principles on AI" (OECD, 2019), "Social Principles on Human-centric AI" (Council for Science, Technology and Innovation, 2019) and "AI Utilization Guidelines" (Ministry of Internal Affairs and Communications, 2019).

[10] When former Foreign Minister Hachirō Arita demanded that novelist Yukio Mishima make an apology ad and provide compensation for damages on the grounds of breach of privacy in the novel "After the Banquet," the Tokyo District Court recognized the legal protection and rights against reckless disclosure of the privacy of the plaintiff and ordered suspension of privacy infringement and recognized the right to demand compensation for emotional distress.

[11] There has been a case of forecasted results based on a data analysis being utilized by a business enterprise, raising concerns over the possibility that it affected the recruitment

On the other hand, the installation of conventional security cameras (cameras strictly for recording captured images) with certain considerations in commercial shopping districts, commercial facilities, public transit systems, etc., in Japan have been accepted positive in some cases. However, caution and concern have been expressed regarding security camera installations with a facial recognition function. In Europe and the United States, regulations are being developed regarding such uses. In Japan, a report regarding camera image use for the assurance of safety and crime prevention was published.[12]

In such a way, adverse impacts relating to privacy are diversifying, combined with the rapid speed of these swift changes in technology, from the breach of personal privacy to adverse social influences stemming from its effects on individuals (social disjuncture, etc.), including the possibility of manipulating public office elections. Furthermore, difficulties in dealing with issues associated with privacy can be attributed to the fact that the concept of privacy is not consistent, such as the variability of each individual's perceptions and social acceptance, depending on context and the passage of time.

In the current age, the concept of privacy can change and the types of issues regarded as associated with privacy are expanding in scope as individuals and

process. Overseas, there is a case of the results of psychological profiling from personal information on social media, thus possibly affecting voting behavior via social media.

[12] In Europe, the Guidelines on the Processing of Personal Data Through Video Devices Version 2.0 was adopted in January 2020. The Guidelines cover the handling of camera images and use of facial recognition technology under General Data Protection Regulations (GDPR). When it was proposed initially, it included regulations that appear to be strict from the standpoint of business enterprises. In the process of publication of "On Artificial Intelligence — a European Approach to Excellence and Trust," a white paper on European artificial intelligence strategy published in February 2020, there had been changes in the description of the use of facial recognition, suggesting vacillation regarding determination of the technology's position. In the United States, regulations prohibiting the use of facial recognition by 53 police and other municipal organizations and the use of information obtained via facial recognition technology were issued in June 2019. There have been companies announcing the suspension of supplying facial recognition software. In Japan, the study group on use of camera images for crime prevention and assurance of safety which was organized by the Personal Information Protection Commission (PPC) conducted deliberations, and published "The Use of Camera Systems with a Facial Recognition Function for Crime Prevention and Assurance of Safety" in March 2023.

society raise the issue of whether something is a breach of privacy.[13,14] Unless business enterprises utilizing personal data deal appropriately with the risks that privacy-related issues can cause on individuals and society (hereinafter "privacy risks"), the results may become management risks that adversely affect on their business management.

Business enterprises that utilize personal data must recognize that privacy risks are personal risks before they are business risks and that they are likely to affect the entire society. Privacy-related studies and activities must be consistently integrated into business activities.

This Guidebook recognizes that the adverse effects on privacy, ranging from personal privacy breaches to the adverse social impacts mentioned above, are considered to be privacy issues, and provides information on the actions that businesses utilizing personal data must take to address these issues.

## 2.3. Importance of Corporate Privacy Governance

[13] Refer to Section 5.2 "Identifying Privacy Issues" for privacy issues.

[14] In the time between the publication of Guidebook Version 1.0 (August 2020) and Version 1.3 (April 2023), social conditions relating to privacy have changed dramatically.
In light of the growing alarm over privacy infringements by digital platforms, etc., that handle massive data, legal schemes are being developed and applied in Western nations to assure transparency in handling user information and in improving accountability. In July 2022, the Digital Services Act (DSA) that imposed on online platforms the obligation of assuring transparency in online advertising and an amendment proposed on the Digital Markets Act (DMA) regulating the "gatekeeper" that satisfies the criteria for providing marketplaces, etc., so as not to set unfair conditions and prevent actions that erode the openness of the digital market (including regulation on combination of personal data among multiple services, etc., on data portability and on audit of profiling technology, etc.), have been adopted by the European Union Parliament. In the United States, a referendum on the amendment of the California Consumer Privacy Act went into effect in January 2020 and its replacement by the California Privacy Rights Act (CPRA) was passed in November 2020. The amended law is scheduled to take full force in January 2023. The CPRA allows the right to opt out of personal data sharing (not only for selling), further strengthening privacy protection.

At the same time, platform operators have started to block or curb cross-site tracking, spurred by the rise of privacy awareness. Apple, which holds a major share in the mobile market, has been implementing the control of third-party cookie use for Safari in phases. Third-party cookies have been completely blocked since 2020. Since April 26, 2021, Apple has also denied use of Identifier for Advertisers (IDFA), the advertising ID provided by Apple, unless that user provides consent, thus imposing significant restrictions on tracking on its app. Google has also announced that it intends to begin phasing out third-party cookies in Chrome in the second half of 2024. Source: "Expanding testing for the Privacy Sandbox for the Web," (Google LLC, July 2022) https://blog.google/products/chrome/update-testing-privacy-sandbox-web/

In many cases, business enterprises functions as the driving force in creating innovation through personal data utilization and in creating value for society. For this reason, business enterprises are expected to play a central role in addressing privacy issues. If appropriate actions are not taken to reduce the potential for privacy issues, personal privacy will be violated. In addition, this may lead a sense of mistrust toward data utilization throughout society, along with anxiety and concern regarding personal privacy risks. Eventually, this will lead to hindrance of innovation. Under such conditions, the realization of Society 5.0, that is, development of a human-centered society that realizes both economic growth and resolution of social issues, become dubious. Hence, action on privacy issues is important and essential in creating Society 5.0. In handling privacy issues, business enterprises must recognize that what they handle through cyber space is not just data and that they are in fact interacting with actual individuals in physical space. Businesses are required to pay strict attention to their actions so as to not compromise the basic rights of the individual, and to respond appropriately.

Additionally, there is a growing movement demanding the corporate responsibility to respect human rights from the perspective of corporate social responsibility and the Guiding Principles on Business and Human Rights.[15,16]

---

[15] In the international sphere, Guidance on Social Responsibility (ISO 26000:2010) and the UN Guiding Principles on Business and Human Rights (United Nations Human Rights Council, 2011) have been adopted. In Japan, the National Action Plan on Business and Human Rights (2020-2025), based on the UN Guiding Principles, was adopted in 2020 by the Inter-Ministerial Committee for Japan's National Action Plan on Business and Human Rights. To boost corporate action with respect to human rights, Report on Research on Business and Human Rights (Ministry of Justice 2021) and the Guidelines on Respecting Human Rights in Responsible Supply Chains (Ministry of Economy, Trade, and Industry, 2022) have been adopted and published. The National Action Plan on Business and Human Rights refers to "Human Rights Associated with the Development of New Technologies", such as defamation, privacy infringement and discrimination issues on the Internet and the appropriate use of AI. Report on Research on Business and Human Rights also mentions "human rights issues related to technology and AI" and "privacy rights" as risks that are related to human rights that businesses must take into account and human rights related to corporate activity, as well as examples of such risks.

[16] In Japan, ESG investment is also spreading. It takes into account not only on conventional financial data but also on environmental, social and governance elements at decision-making on business investments. ESG investment is expected to contribute to the achievement of the sustainable development goals (SDGs) adopted by the United Nations in 2015. (Reference: The Government Pension Investment Fund (GPIF) website: https://www.gpif.go.jp/esg-stw/esginvestments/.)

The Stewardship Code (Financial Services Agency, revised in 2020) and the Corporate Governance Code (Tokyo Stock Exchange, Inc., revised in 2021) also mentions the importance of the assessment of the status of investment recipients and of disclosure of corporate

Corporate efforts to not compromise the basic rights of individuals and consumers and to take appropriate actions, including the development of internal schemes and systems, to correct and prevent the occurrence of privacy issues also are consistent with such social demands.

At present, the principal normative in handling privacy problems in Japan is the APPI. For this reason, corporate concern in conducting business with attention to privacy issues has been centered on compliance with the APPI until now, and in many cases, such concerns have been central in review of business operations. Also, with changes in terms of spectacular speed and technological innovation, the emergence of new privacy issues and the rise in privacy awareness among people, these issues have not necessarily been limited to the scope of compliance with the Act but also reflect doubts in business enterprises from the viewpoint of social acceptance and cases of social media "flaming" resulting from business enterprises being unable to avert criticism related to privacy issues. Unless they are able to prevent the occurrence of privacy issues related to individuals or to society, business enterprises may face injunctions or demands for compensation for damages, or may lose trust in society[17]. Business enterprises are now urgently required

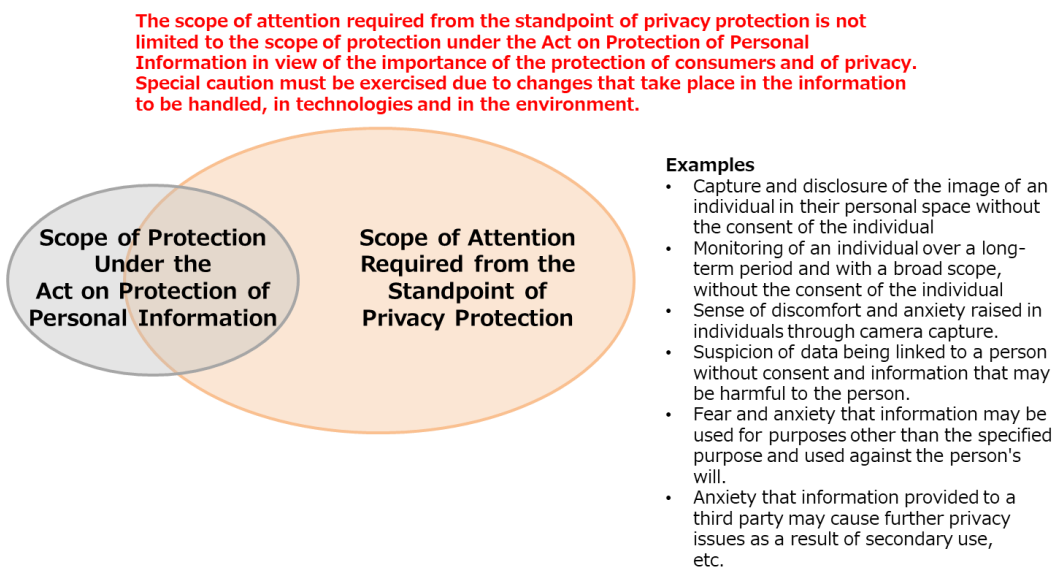
---

information from the viewpoint of promoting sustainability-related activities, including ESG elements. In ESG investment, human rights are regarded an important element in the social arena and are growing in attention in the dialogue between institutional investors and business enterprises and in the disclosure of nonfinancial information by business enterprises. Global Reporting Initiative (GRI) standard that is one of the frameworks in ESG information disclosure includes items on disclosure relating to customer privacy as an option that business enterprises are free to choose. There are cases of privacy and data security included as one of the key issues in ESG pointed out by ESG rating agencies (e.g., the MSCI ESG Ratings model). In the coming years, winning recognition from both investors and society through information disclosure in the form of integrated reports, etc., and dialogues with markets is expected to become increasingly important in addressing privacy issues.

[17] "The Use of Camera Systems with a Facial Recognition Function for Crime Prevention and Assurance of Safety" (PPC, 2023) illustrates that court cases on disputes regarding the rights of image and privacy in Chapter 4 (Points of Note in the Right of Image and Privacy), and in section 2 (Success or Failure of Torts and Their Relationship with APPI), regarding the relationship between the shooting by using a camera system with a facial recognition function, and Tortious Acts and APPI, it sets forth that “the tort law and APPI have different purposes and characteristics, therefore when a tortious act is conducted, it may constitute a violation of APPI at the same time, however, it may not necessarily constitute a violation of APPI”, and that “the factors which are taken into account in assessing whether or not a tort regulated under the Civil Code has been committed should be taken into consideration in the interpretation of provisions of APPI on prohibiting inappropriate use (Article 19) and on proper acquisition (Article 20-1)” considering that APPI pays attention to the rights and interests of individuals by taking into account the nature and the handling method of personal information and trend of court cases on disputes regarding the rights of image or privacy.

to not just superficially comply with laws and regulations, but to take voluntary action and give explanations considering their impacts on the rights and interests of individuals and to the social values based on how personal data is utilized in their business.

**Figure 3. Scope of Attention Required from the Viewpoint of Privacy Protection (image)**




Notwithstanding, a look into the issues that business enterprises face, based on events that have invited criticism in recent years, shows that legal compliance is positioned at the center of action in Japan. As the term "compliance" suggests, action is passive in a certain sense, and the focus has been inclined to be on case-by-case actions to conform with laws and regulations. Today, there is little awareness toward the fundamental purpose (i.e., preventing privacy issues) behind a case-by-case response. Against this backdrop, action on privacy issues is itself perceived as compliance cost. There are instances of businesses trying to "rationalize" this to the greatest possible extent within the scope of legal compliance. When flaming occurs[18] in the course of such action, business enterprises end up wondering why this is so in spite of their compliance with the law. As a result, this may incite a vicious cycle of the business enterprise suffering losses and to the business enterprise becoming more conservative and reluctant to utilize personal data.

[18] As mentioned earlier, social media flaming occurs not only within the scope of legal compliance but also from the perspective of social acceptance.

Under these conditions, there are quite a few business enterprises in Japan and other countries that have been able to expand into new business fields by utilizing personal data while gaining the trust from customers and consumers. These companies do not perceive privacy-related activities as mere compliance but part of an important management strategy. Through the appropriate handling of privacy issues, they are succeeding in gaining social trust and in upgrading their corporate value.[19] In particular, reducing privacy risks associated with products and services of the company and fostering greater affinity with ensuring privacy will lead to the company gaining the trust from society, including consumers. For this reason, all business enterprises must not view privacy-related activities as a cost but revamp their perspective as a way to enhance the quality of their products and services and thus boost corporate value.

With the great speed of change taking place today, businesses must not only pay adequate attention to legal compliance but engage in risk management and activities aimed at gaining social trust. For this purpose, businesses must actively communicate with consumers and stakeholders and respond proactively to privacy issues while conforming to legal compliance in the narrow sense. In other words, business enterprises establish what actions they take (code of conduct) based on dialogues with consumers and other stakeholders and adhere faithfully (comply) with the rules. Business enterprises then disclose (explain) these actively to society, and gain trust through dialogues with consumers and other stakeholders. Business enterprises are required to make the transition in their organizational stance toward a "comply and explain" style on a company-wide basis. Moreover, the business enterprise must not only comply with the code of conduct once established but continue to review and re-examine the best possible solution

[19] For example, Apple announced four principles on privacy protection and policies on improving tracking transparency, etc., in April 2021.

based on the business enterprise's goals and the ever-changing environment.[20,21,22]

[20] The Japanese government has been providing support to business enterprises in the past in addressing privacy issues to promote personal data utilization. In particular, the working group on promoting data distribution established under the IoT Acceleration Consortium and managed jointly by the Ministry of Economy, Trade and Industry and the Ministry of Internal Affairs and Communications has been providing counseling to individual business enterprises, offering expert advice in dealing with privacy issues that have become problems in each company's business operation. At the same time, information collected has been compiled in "Case Studies on Review of the New Form of Data Distribution Trade." It has not provided beneficial information to business enterprises. (Version 1.0 published in 2017 and amended as Version 2.0 in 2018.) After the release of Version 2.0, the working group has continued conducting reviews and has published its first volume. It is scheduled to add case studies each year.

In addition, the "Guidebook for Utilization of Camera Images" has been published and updated since 2017 to promote utilization of camera images that are highly likely to be utilized in view of their characteristics. The Guidebook organizes matters to be taken into account by business enterprises in protecting the privacy of consumers and engaging in appropriate communication. (Version 1.0 published in 2017, followed by amendments to Version 2.0 in 2018 and to Version 3.0 in 2022.) In addition, the "Guidebook for Utilization of Camera Images: Collection of Samples Pertaining to Advance Reporting and Notification" (2019) and "Matters of Concern in Action by Private Business Operators for Public-Interest Purposes Utilizing Camera Images: Study in Cases of Infection Countermeasure Use" (2021) have been published. Underlying these actions is, compliance with the APPI as a matter of course, but these actions are not limited to offering necessary advice on statutory compliance but also providing counseling and information to enable business enterprises to address privacy issues on a higher level. However, the actions until now have been providing advice on specific actions to be taken by a specific business. To implement broader and more general action to support transition in business enterprises' organizational stance toward a "comply and explain" style, the study group on corporate privacy governance model was created under the working group on promoting data distribution for further review.

[21] "GOVERNANCE INNOVATION: Redesigning Law and Architecture for Society 5.0" (Ministry of Economy, Trade and Industry, 2020) also indicates the need for corporate comply-and-explain.
https://www.meti.go.jp/press/2020/07/20200713001/20200713001-2.pdf
"GOVERNANCE INNOVATION Version 2: A Guide to Designing and Implementing Agile Governance" (Ministry of Economy, Trade and Industry, 2021) indicates that the governance model in Society 5.0 that is to be found for the sophisticated integration of diverse, complex systems in cyber space and physical space requires continual review into the most optimal solutions, vis-à-vis the goals and the ever-changing environment.
https://www.meti.go.jp/press/2021/07/20210730005/20210730005-2.pdf
"Agile Governance Update" (Ministry of Economy, Trade and Industry, 2022) was published as a commentary to elucidate the two reports on governance and innovation mentioned above and unified form.
https://www.meti.go.jp/press/2022/08/20220808001/20220808001-b.pdf

[22] When promoting innovation by utilizing AI, the business enterprise is required to respect the principles of AI and to adopt a risk-based approach controlled to correspond to the scale of risk AI holds. In this study into the scope of AI's influence, privacy protection becomes an important perspective.
"AI Governance in Japan Version 1.1 — Report of the Expert Group on How AI Principles Should be Implemented" (Ministry of Economy, Trade and Industry, 2021)

In view of these circumstances, the basic concept of corporate privacy governance is that business leaders actively engage in activities relating to privacy issues, develop a system across the organization for addressing privacy risks, and make the system work, in order to ensure the proper risk management of privacy issues and assurance of trust, and to ultimately upgrade corporate value.[23]

Generally, governance in business enterprises calls for business leaders to "direct" from the viewpoints of management strategy and risk management, along with those business activities for achieving policy direction. Business leaders also are to "monitor" the state of such activities and "evaluate" them to determine the results obtained *vis-à-vis* this policy direction. Governance is implemented when this basic cycle of setting the direction, monitoring and evaluating is functioning.[24]

In privacy governance, business leaders also take action based on the value that is to be provided by the company through its personal data utilization, regarding its statutory compliance as a matter of course. Business leaders likewise "direct" by stating explicitly the fundamental approach to organizational privacy protection and the stance in responding actively to manage such risks that privacy issues may cause for individuals and society (privacy risks). This is based on the value that is to be provided by the business enterprise through its personal data utilization, in addition to its statutory compliance. Business leaders are to “monitor” privacy risk management activities aimed at this policy direction, etc., “evaluate” the findings *vis-à-vis* the substance of the privacy governance stated explicitly and " direct" again based on the evaluation findings. It is useful to have the

https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_8.pdf
"AI Governance Guidelines for Implementation of AI Principles Ver. 1.0" (Ministry of Economy, Trade and Industry, 2021)
https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_9.pdf

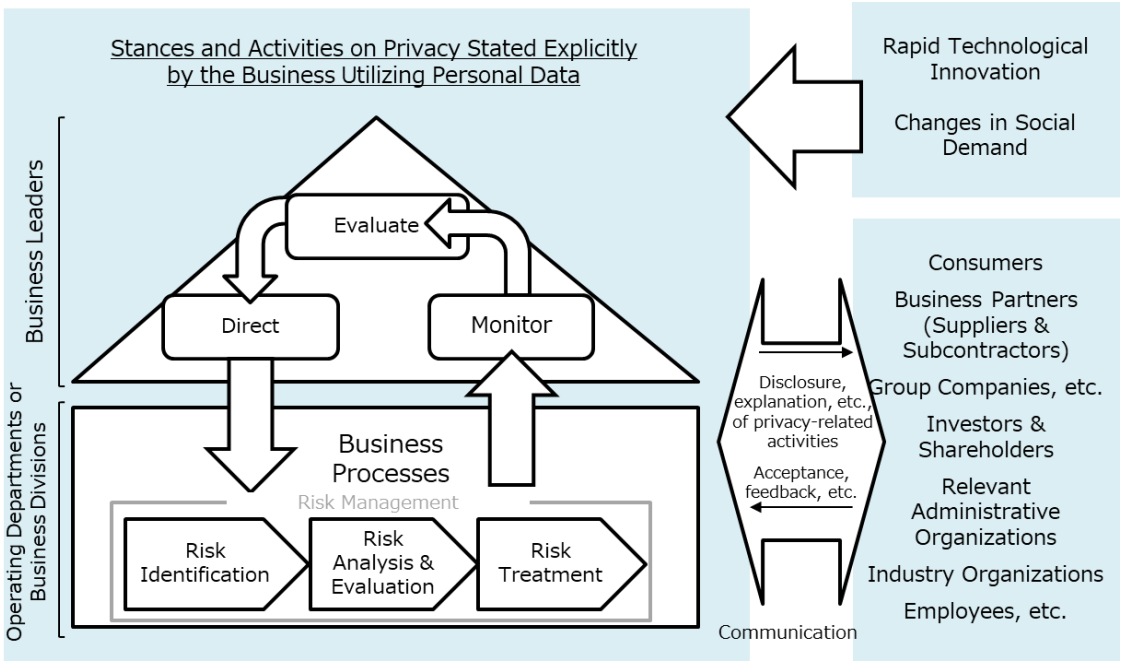
[23] Japan Business Federation (KEIDANREN) issued "Management Manifesto on Proper Utilization of Personal Data" in October 2019 and urged business leaders to recognize that measures for personal data protection and cybersecurity not only reduces business risks but secures the safety and security of individuals and therefore contributes to the creation of corporate value in the longer-term perspective.

[24] Among the various frameworks that organize matters required for corporate governance, the general model that business enterprises can refer to in their drive to implement to DX that brings change into a business model utilizing data and digital technologies and to increase competitiveness is IT governance (ISO/IEC 38500).

cycle as described above work. Furthermore, risk management is generally executed by identifying the risks in business processes such as service and system planning and development, and then operating, analyzing and treating these and taking the appropriate action.

As mentioned earlier, the rapid speed of technological innovation, changes in the external environment including social demand, etc., and the constant change taking place in the concept of privacy (differences in perception of privacy by individual, variability of social acceptance for privacy depending on context and the passage of time, etc.) make it necessary for businesses to gain trust through an explanation of their activities through communication with consumers and other stakeholders and to improve their activities continually, based on concerns and feedback associated with privacy.[25]

**Figure 4. The Framework of Privacy Governance**

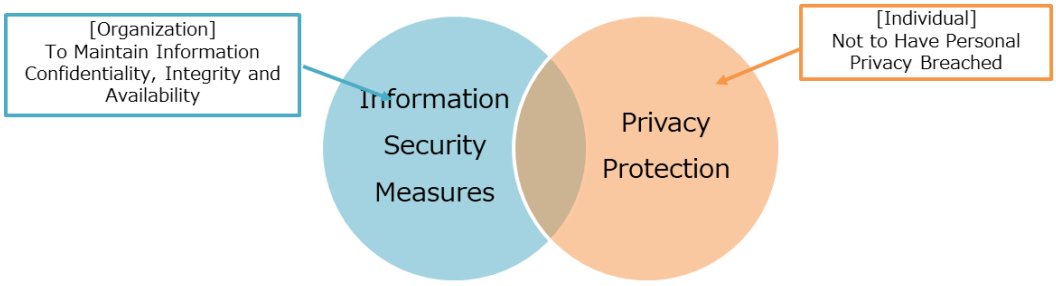



[25] The approach to governance in business enterprises differs by individual business enterprise. Figure 4 shows general framework of privacy governance. On the assumption that the illustrated cycle is functional in governance in business enterprises, this Guidebook organizes specific matters that should be implemented from the viewpoint of privacy in the course of developing governance functions and risk management processes in business enterprises for building corporate privacy governance.

Column: Information Security Measures and Privacy Protection

Although information security measures and privacy protection are both essential in the DX age, the two differ in concept. The objective of information security measures is the maintenance of confidentiality, integrity and availability of information that is the company's asset. In contrast, privacy protection requires appropriate actions by the business enterprise so as not to compromise the privacy and other basic rights of the individual. For this purpose, it is necessary to identify, analyze, and evaluate not only information security measures but also projected privacy risks in the broader sense (for individual consumers and for society, in some cases). In particular, communication with consumers is essential in appropriate risk identification, analysis, and evaluation.

In consumer privacy protection, it is important to implement appropriate information security measures to protect consumer personal data. However, there are cases of conflict between information security measures and privacy protection, such as excessive surveillance of employees to assure the confidentiality of information that makes up the company's assets.



## 3. The Three Requirements to Be Addressed by Business Leaders

To realize Society 5.0, business enterprises are expected to play a central role in creating innovation through data utilization. In a society founded on data utilization, maintenance of a consistent stance to protect consumer privacy leads to the enhancement of the quality of the products and services in each business enterprise, gaining advantage in business, gaining the trust from consumers and stakeholders, and resulting in an improvement in corporate value. In other words, privacy protection and data utilization should not be perceived as opposites but should be understood from the viewpoint of maximizing the benefit of data utilization while paying due attention to privacy. It is important for business leaders, for example the top management and executives, to consider privacy-related activities as part of management strategy and study it as a factor in competitiveness.

If a business enterprise is unable to deal with privacy risks or to prevent the occurrence of privacy issues related to individuals or to society, it may face injunctions or demands for compensation for damages (Article 709 of the Civil Code), or it may lose trust in society. Such a situation will not only have an adverse impact on its sales and profits but also raise concerns over whether the business is able to maintain its operations or even survive. Business leaders need to take action to address such possibilities.

Business leaders of a business enterprise owe the duty of care of a good manager. This responsibility includes the development of a risk management system according to the scale of the business enterprise. For this reason, compensation for any losses incurred as a result of inadequacies in the system must be covered not only by the executive officers responsible for the relevant department but other executives as well.[26] For a business enterprise promoting DX, the proper management and utilization of personal data are important in its business operations. If appropriate internal control has not been developed and the business suffers damages as a result of information leakage or flaming, attention must be paid to the fact that the business

[26] Article 423 (Liability of Officers to Stock Company for Damages) and Article 429 (Liability for Damages of Officers to Third Parties) of Companies Act and Article 709 (Compensation for Loss or Damage in Torts) of Civil Code.

leaders will be held responsible individually for the compensation of losses.[27,28]

In view of these conditions, business leaders are required to consider privacy-related activities as a crucial element of corporate competitiveness and address these activities as important issues in their management strategy. And at the same time, they are required to implement corporate governance, along with the development and operation of an internal control mechanism to support them.

To implement privacy governance, business leaders are required to begin by fulfilling the following three requirements.

| |
|---|
| Requirement 1: Explicit statement of the corporate stance on privacy governance.<br>Requirement 2: Appointment of the Officer Responsible for Privacy Protection.<br>Requirement 3: Investment of resources in privacy-related activities. |

## 3.1. Explicit Statement of the Corporate Stance on Privacy Governance

To create value through innovation with data utilization under the business enterprise's corporate philosophy, the protection of consumer privacy with consistency in the corporate stance leads to improve the quality of its products and services, etc., and to gaining trust from consumers and society. It will also lead to enhance corporate value.

Business leaders need to recognize this as one of the important management issues and state explicitly their basic policy focused on privacy protection that enables their organization to maintain consistency in its handling of such matters, as well as its stance in responding actively to

[27] Although the executive officer as an individual is not necessarily held liable for all flaming incidents, if the company requires measures to prevent such incidents as part of proper risk management system to protect personal data held by the company and other forms of data use and flaming occurs as a result of failure to develop such a system, the officer may be held liable as an individual on the grounds of violation of the obligation to develop an internal control system.

[28] For this reason, there is a growing number of outsourcing enterprises, such as cloud service providers, that are seeking the assurance of trust by obtaining an internal control assurance report relating to security, availability, integrity or processing, confidentiality and privacy regarding their services (known as a SOC2 report).

privacy risk management. Business leaders also need to communicate awareness of the corporate policy and their stance both inside and outside of their organization. The above should be undertaken with consideration as to what kind of value the corporate enterprise has to offer through its data utilization.

Through top-down dissemination of this policy direction, the awareness can take root throughout the organization. In addition, announcement of the policy and outlook not only within the organization but also to external parties such as consumers and stakeholders (shareholders, business partners, etc.) will serve as foundation for building trust. Business leaders are required to ensure accountability[29] for implementing privacy-related activities based on the announcement that has been explicitly made. [30] This explicit announcement may take the form of a privacy statement issued as a declaration or behavioral principles that apply to the entire organization.[31]

[29] Accountability refers not just to the responsibility of providing an explanation but the establishment of conditions that enable the organization to fulfill comprehensive and ultimate responsibility.

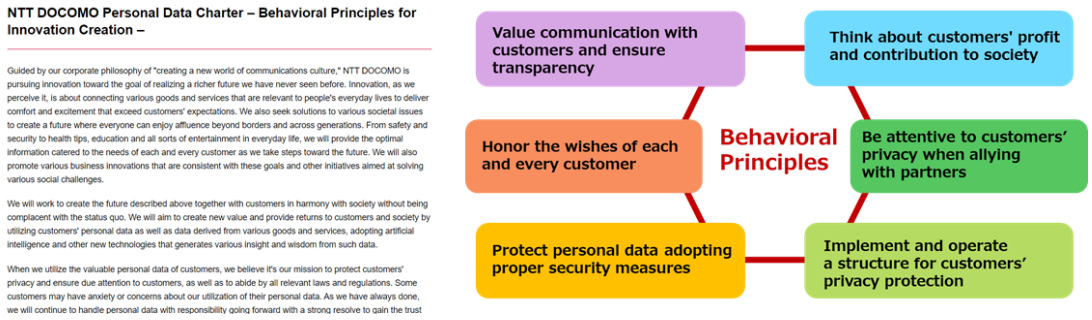
[30] Production of an explicit statement of the corporate stance involves the concept called Privacy by Design (PbD), one of the global standards that serve as reference as the basic approach to privacy protection. Each time a privacy issue emerges in business or in an organization, the response to privacy risk should be planned not simply as a stopgap measure. Rather, the concept calls for privacy protection to be taken into account from the initial stages of design in business development. The PbD approach and one of the foundational principles of PbD (see Chapter 7 "Privacy by Design of this Guidebook") — "positive-sum, not zero-sum" — is a useful reference for business leaders in establishing its stance on privacy governance since they are highly compatible and consistent with the role of the business enterprise and an explicit statement of corporate stance.

[31] Many business organizations issue a document entitled "Privacy Policy." Very often, they have been issued in compliance with the "3-6 Approach and Policy in Promoting Personal Information Protection" of the Guidelines on APPI(General Principles)" or the internal policy on personal information protection and external policy on personal information protection specified as requirements in JISQ 15001:2017 Personal Information Protection Management Systems - Requirements. The key is that, regardless of format, the message expressing the strong determination of business leaders is issued explicitly.

**Example: Publication of NTT DOCOMO Personal Data Charter**

NTT DOCOMO, Inc., has developed and published the "NTT DOCOMO Personal Data Charter - Behavioral Principles for Innovation Creation". It announces the following; Guided by corporate philosophy of "creating a new world of communications culture", NTT DOCOMO is pursuing innovation toward the goal of realizing a richer future we have never seen before. NTT DOCOMO is working to create the future described above together with customers in harmony with society without being complacent with the status quo. And when NTT DOCOMO utilize the valuable personal data of customers, it is believed that to protect customers' privacy and ensure due attention to customers, as well as to abide by all relevant laws and regulations, is own mission.

Therefore NTT DOCOMO has set forth six principles as behavioral principles.




Source: https://www.docomo.ne.jp/english/utility/personal_data/charter/?icid=CRP_en_UTI_privacy_txt02_to_CRP_en_UTI_personal_data_charter

To consider advances in technology and societal demands, it is necessary that the substance and operation of the behavioral principles and policies on conduct are revised continuously and modified appropriately to respond to and gain trust from society.

## 3.2. Appointment of the Officer Responsible for Privacy Protection

Privacy governance requires the intervention of business leaders and concrete action in line with the content of the statement issued explicitly on privacy governance (see Section 3.1). For this purpose, business leaders need to appoint a person to take charge of privacy-related activities across their organization as the executive officer in charge (hereinafter "Officer Responsible for Privacy Protection") of executing the responsibility to implement what business leaders stated explicitly as their corporate stance. To monitor that the content of what business leaders stated explicitly is being implemented, business leaders require the Officer Responsible for Privacy Protection to make reports on risk management activities, etc., in the

business processes of service and system planning, development and operating and to evaluate the content of the report with their statement. Based on the findings, business leaders are to set their policy direction for internal controls and make them work effectively (see Page 18). To do so, it is necessary to clearly identify the scope of responsibility of the Officer Responsible for Privacy Protection and to grant the officer authority for executing the countermeasures to appropriately prevent privacy problems from arising. In view of the privacy risks in the business enterprise, the distinctive features of its organizational structure and smooth business operations, etc., business leaders should appoint a person with the appropriate job status, as the Officer Responsible for Privacy Protection.[32] [33,34,35]

[32] Regarding the Officer Responsible for Privacy Protection, titles such as "manager", “director", and "senior" may be used instead of "officer" depending on the type, scale, and region of the business enterprise.

[33] The office of the Officer Responsible for Privacy Protection should in some cases be taken by an executive officer with the authority to be involved in decision-making on the purpose and means of personal data processing within the organization for the Officer to function effectively.

[34] 3-3-2(3) of APPI "The Every-Three-Year Review" Outline of the System Reform specifies that "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."

[35] General Data Protection Regulation (GDPR) obliges the appointment of a Data Protection Officer (DPO) who is guaranteed a strong level of independence in the provision regarding conflict of interests. The DPO cannot be appointed to a job rank (senior management positions, etc.) that leads to decision-making on the objectives and methods of personal data handling within the organization.

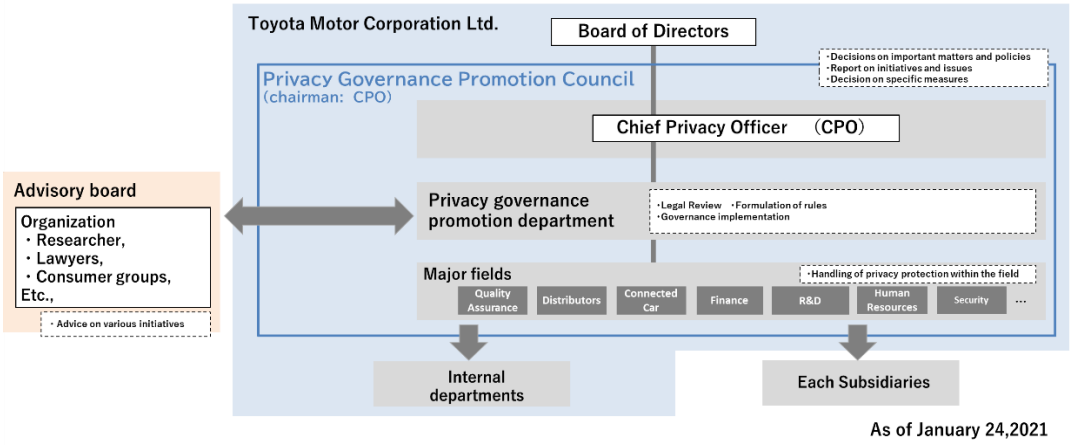
In the United Kingdom, the appointment of a DPO is provided for in the UK General Data Protection Regulation (UK GDPR). However, the appointment provision has been re-examined in view of the problems in such an appointment, especially in a small-scale organization. Deliberations of the Data Protection and Digital Information Bill are underway for the possible appointment of a senior responsible individual in senior management to take charge of handling data protection risks in the organization.

## Example: Appointment of Chief Privacy Officer (CPO) at Toyota Motor Corporation

Toyota has established a company-wide cross-sectional governance system to achieve respect for privacy of customers and appointed the Chief Privacy Officer (CPO). Under the control of CPO, managers for privacy protection are assigned for each major business field (quality assurance, distributors, Connected Car, finance, R&D, human resources, security, etc.) and their corresponding privacy risks.

In addition, the privacy governance promotion council chaired by the CPO is to convene regularly to share and review matters pertaining to privacy protection action in each field, issues pertaining to privacy shared by all companies and important matters including communication with consumers. When important privacy-related incidents occur, privacy governance promotion department that received the report from a business department or division quickly identify the incidents, report them to the CPO and management executives and then take countermeasures.

In addition, an advisory board composed of external experts have established and are working to build a system that incorporates the perspective of a third party to ensure that privacy is appropriately considered.



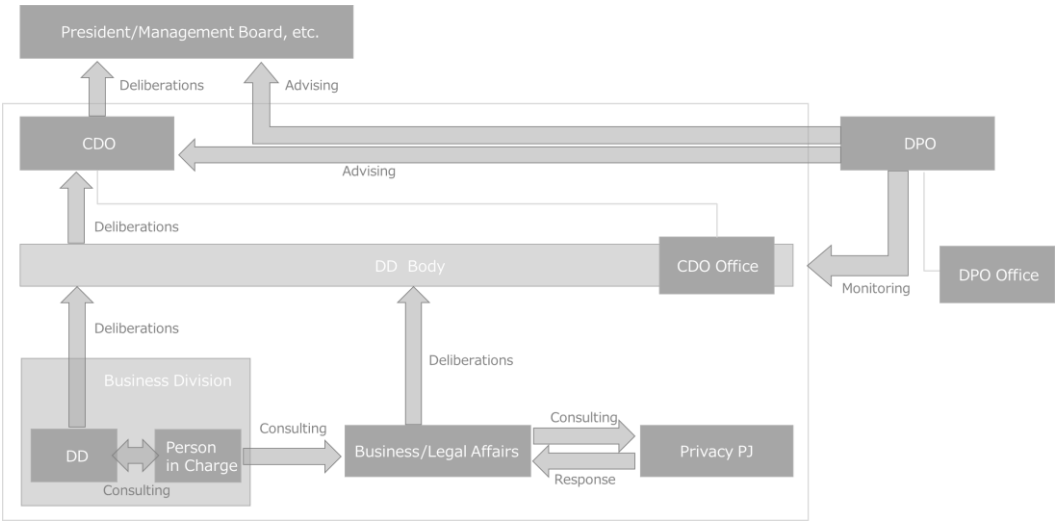

Source: https://global.toyota/en/sustainability/privacy/initiatives/

**Example: Appointment of the Chief Data Officer (CDO) and Data Protection Officer (DPO) at Yahoo Japan Corporation**

Yahoo Japan Corporation has appointed its CDO (Chief Data Officer) in order to promote data utilization in compliance with laws and with attention to privacy. Under the CDO, the DD (Data Director) to deal with both data utilization and privacy protection is appointed for each service. Furthermore, the DPO (Data Protection Officer) is appointed to provide counseling, surveillance and evaluation of propriety in data protection handling from an independent standpoint and from the perspective of the user and society.

In handling privacy protection pertaining to business projects, the person in charge in the business department consults with the legal affairs division. The person in charge of legal affairs consults with the privacy handling team within the division as needed, which in turn reviews and gives response on the issue. The DPO examines into the decision-making process and determines whether it is appropriate.

For business projects that affect the entire business group, the DD body comprising the DDs representing each service conducts a review and consults the CDO regarding the matter. The DPO provides the necessary advice for the CDO to make appropriate decisions.




Source: Internal reference materials

## 3.3. Investment of Resources in Privacy-Related Activities

To put the corporate stance stated explicitly into action, business leaders are required to invest the necessary and adequate quantity of management resources (people, goods, money, etc.). It is necessary to establish a system aimed at taking an active response to privacy risks associated with personal data utilization in the business enterprise, and to allocate adequate manpower and assure human resource development, including manpower recruitment.

Privacy-related activities should be studied beforehand and integrated into business strategy, operations, and systems.[36] In addition, privacy risks may occur under normal conditions and are not necessarily dependent on business management conditions or the external environment. For this reason, it is expected to invest resources continually in dealing with privacy, for extending continuity of these activities.

It is also necessary for business leaders to monitor the results of the resource investment, evaluate whether additional investment is necessary etc., and take action based on the evaluation results, etc., in defining the next policy direction (and to execute this process repeatedly). An explanation of these activities should also be given to outside parties.

[36] The philosophy underlying PbD and its 7 Foundational Principles (Proactive/Preventive and Privacy as the Default Setting etc., in Chapter 7 "Reference: Privacy by Design" in this Guidebook) serves as a reference.

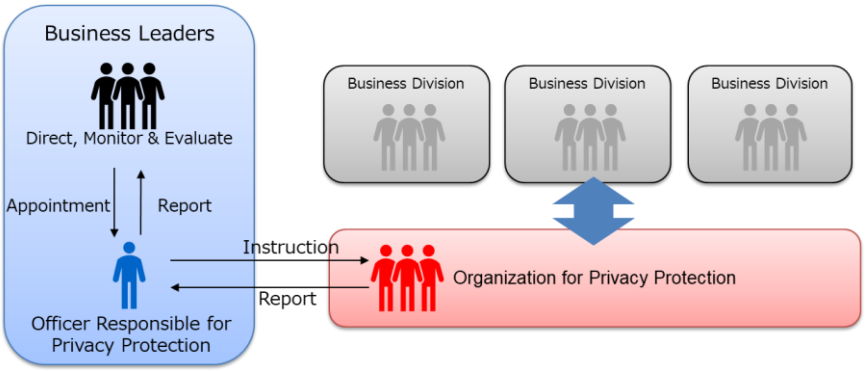
# 4. Key Items in Privacy Governance

## 4.1. Establishing a System for Privacy

Business enterprises that utilize personal data need to aggregate information from their business divisions, uncover all privacy risks in the divisions, and makes privacy governance work. Based on the findings, it is necessary to execute privacy risk management for a multiple sided study into measures in handling such risks. The functions in risk management, that is, risk identification, analysis and evaluation, treatment and continual review and updates, need to be implemented inside enterprises' organizations themselves.[37,38]

To realize the above, it is desirable for business leaders to establish an organization led by the Officer Responsible for Privacy Protection (hereinafter referred to as the "Organization for Privacy Protection") inside the business enterprise.

**Figure 5. Establishment of a System for Privacy Protection**




[37] Privacy risk is identified, the possible result or likelihood of occurrence of the identified risk analyzed, the level of importance in handling the risk is evaluated vis-à-vis the corporate stance relating to privacy governance stated explicitly by business leaders and the decision is made on management method and counteraction. The results of the action should also be reviewed for improvement.

[38] Reference materials on risk management method are JIS Q 15001 (Personal Information Protection Management Systems), which lays the foundation of compliance with the APPI in Japan and, in the international arena, ISO/IEC 27701, which is an extension of ISO/IEC 27001 and ISO/IEC 27002 to include information security management systems which provides the requirements and guidelines to protect privacy that is likely to be affected by personally identifiable information (PII). These management system standards have been systematized and serve as reference. ISO/IEC 27001 and ISO/IEC 27002 have been published as JIS standards, namely, JIS Q 27001 and JIS Q 27002. ISO/IEC 27701 is also expected to be published as a JIS standard in the future.

The rapid pace of technological innovation and increasing consumer awareness toward privacy have steadily expanded of the scope of matters to be examined from the viewpoint of privacy protection. For this reason, establishment of an Organization for Privacy Protection is needed to address privacy risks through multiple sided review and an agile response to technological innovation, social demand, consumer awareness, etc. In addition, to deal with the personal data of consumers, etc., on a global scale, it is also necessary to pay adequate attention to the application of various foreign laws and regulations and establish an organizational system for privacy to globally deal with privacy protection.[39,40]

Although the number of business enterprises with an Organization for Privacy Protection is not many at present, the establishment of such an organization will build a network with related business divisions and departments, including the new business division, and cultivate closer communication. This also will enable them to promote concrete action, such as the collection, accumulation and sharing of relevant information and knowledge from external experts, etc., within the business enterprise, and reviews into multiple sided measures to address privacy risks, etc.

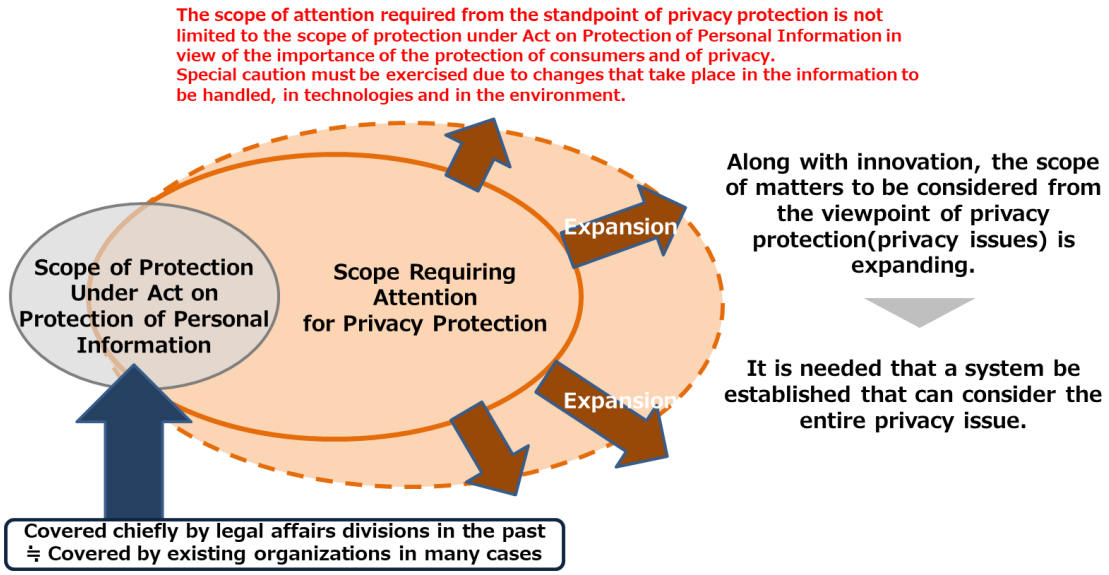
Business leaders should establish the system by assigning the privacy risk management function and key role in privacy-related activities to an appropriate department or division, etc., with attention to the business enterprise's own privacy risks, the distinctive features of its own organizational structure and climate (including the characteristics, roles,

[39] In the 2020 amended APPI, the provision of personal data to third parties located in foreign countries with consent of the identifiable person requires that the information provided to that person be amplified (the name of the foreign country, information on the personal information protection system of the foreign country, and information on the measures the third party takes for the protection of personal information). When providing personal information without the consent of the identifiable person, on grounds that the foreign third party has established a system that conforms to standards prescribed by Order of PPC, execution of certain measures to the third party, such as the routine check and response in the case of an incident, is required. Additionally, the businesses handling personal information is required to make the information about the personal data they hold accessible to identifiable persons, regardless of whether personal data is to be provided to third parties located in foreign countries. An example of the information which is accessible to identifiable persons as the necessary and appropriate measures for managing the security of personal data is the implementation of safety controls founded on an assessment of the personal information protection systems and schemes in foreign countries where the personal data is to be stored.

[40] Regarding the method of collecting information relating to foreign laws and regulations, etc., see Chapter 6 "Reference: Information Collecting Methods Related to Foreign Laws and Regulations, etc."

relationships, etc., of the existing divisions) and facilitating its business operations, and so on.

**Figure 6. Importance of Establishment a System for Handling Expanding Privacy Issues**



**Example: Santen Pharmaceutical Builds Privacy Governance on a Global Scale**

Santen Pharmaceutical Co., Ltd., is building a global organization for handling personal data. In April 2020, the company adopted a global policy that includes basic rules regarding privacy. Under its global head office, guidance and instructions are issued to each regional and functional head office through the Data Manager.

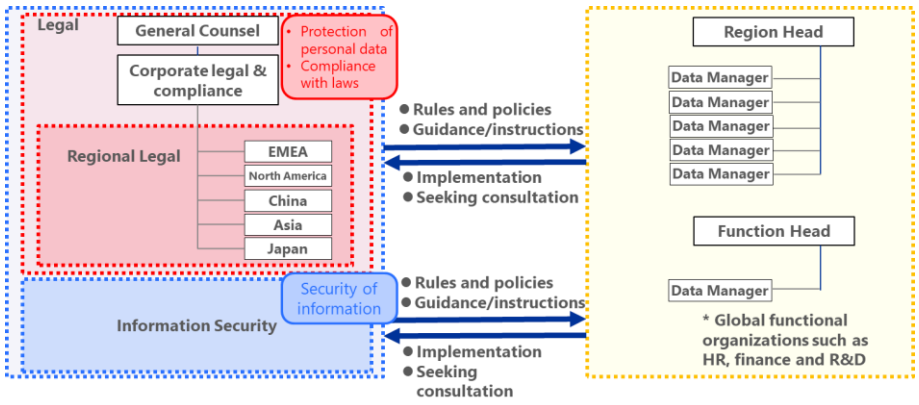
**Agenda and Contents**

- **Chapter 1. General Provisions**
  - Objective, Scope, Definition, etc.
- **Chapter 2. Roles and Responsibilities**
  - Each Division's Roles and Responsibilities
- **Chapter 3. Processing of Personal Data**
  - Privacy by Design, Management of Personal Data, Data Minimization, Recording, Security, Retention Policy, etc.
- **Chapter 4. Rights of the Data Subject**
  - Notice, Rights of Data Subjects, Requests from Data Subject, Responding to Complaints
- **Chapter 5. Data Breach and Reporting**
  - Reporting of Violation (internally and to authority)
- **Chapter 6. Education of Employees**
  - Education on processing personal data within assigned roles and tasks
- **Chapter 7. Miscellaneous Provisions**
  - Amendment, Effective Date

**Chapter 2. Roles and Responsibilities**

- **Chief Administrator**
  (＝Person responsible for Compliance)
  - Oversee across Santen Group
- **Corporate Legal & Compliance Department**
  - Plan, administrate and provide training across Santen Group
- **Regional Legal & Compliance**
  - Guide and provide training to companies in assigned regions in accordance with Group Policy and local laws
- **Member Companies & Divisions**
  - Manage personal data in compliance with the Policy and applicable laws
  - Appoint "**Data Manager**" in each company
    (For global division, CA would judge the necessity of appointment.)
- **Information Systems**
  - Ensure security of personal data across Santen Group

Global Data Privacy Policy / Source: internal Reference Materials

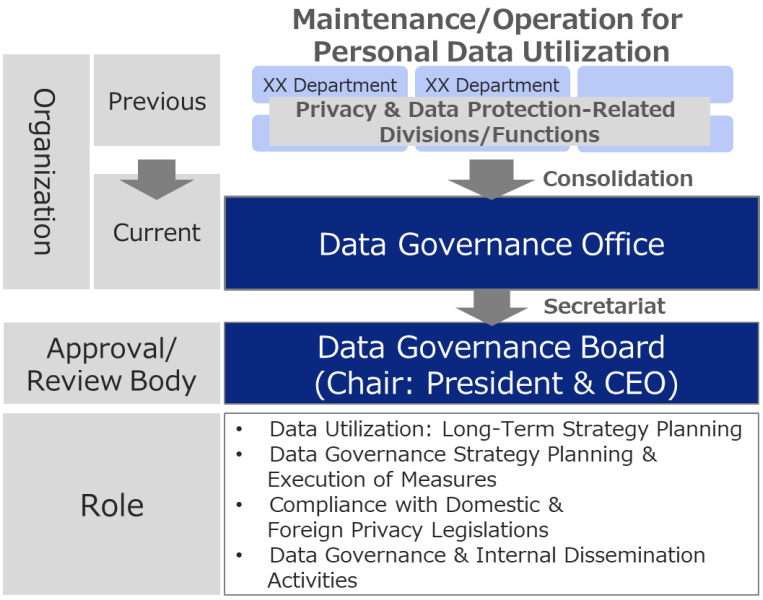



Development of Personal Information Protection System / Source: (internal Reference Materials)

**Example: Installation of Data Governance Office at KDDI**

KDDI Corporation set up its Data Governance Office in FY2020 as a new organization that consolidates and integrates the functions in each organization pertaining to the organization and management of personal data utilization.

The Data Governance Office was positioned as a body headed by the relevant executive officer as its president and is responsible for data utilization and governance strategy planning, etc. The company has also formed the Data Governance Board, the decision-making body on data governance that is chaired by the company president.




Source: Internal Reference Materials

### 4.1.1. The Role of The Officer Responsible for Privacy Protection

The Officer Responsible for Privacy Protection establishes the practical policies based on the corporate stance stated explicitly by business leaders, under its authority granted by business leaders. The Officer Responsible for Privacy Protection is responsible for thoroughly implementing these policies by establishing a system for privacy risk management (to identify, capture, evaluate, and review countermeasures) as part of the business process. The policies are required to include measures for an emergency response if privacy issues have arisen, as well as measures for consumer relief and cause analysis and improvement.

The Officer Responsible for Privacy Protection will report to business leaders, and business leaders will evaluate content of the report based on their explicitly stated stance on privacy governance.

#### 4.1.2. The Role of the Organization for Privacy Protection

The Officer Responsible for Privacy Protection should establish an Organization for Privacy Protection as the core organization to fulfill the actual functions of privacy-related activities. Although the Organization for Privacy Protection should be designed with attention to the importance of privacy governance (see Section 2.3), the actual form is expected to differ by business enterprise. It is important to organize an Organization for Privacy Protection that is effective and adapted to the business enterprise's resources, such as formation of an organization exclusively by employees appointed concurrently, if specialists possessing expert knowledge cannot be recruited for the purpose.

The Officer Responsible for Privacy Protection is required to make the Organization for Privacy Protection well-known throughout the business enterprise.

The primary role of the Organization for Privacy Protection is to identify without fail the risks of privacy issues emerging among consumers or in society through aggregating a variety of information relating to new businesses and services from business divisions within the enterprise or through any other actions.[41] For this reason, it is desirable for the Organization for Privacy Protection to not only accept inquiries related to privacy widely from business divisions, but also have close contact on a daily basis, such as encouraging business divisions to actively share problem awareness, etc.[42] It is important that divisions involved in new business projects or new technology development do~~es~~ not try to tackle issues independently, rather systems and environments should be created to encourage free dialogue and consultation.

Furthermore, relevant information (on market trends, technologies, regulations, etc.) is required to be collected continually~~,~~ in the face of the rapid speed of technological innovation, differences in perception of privacy issues depending on the individual, and changes taking place in social acceptance depending on context and the passage of time. It is also necessary to build

[41] See Section 5.2 "Identifying Privacy Issues" for matters related to privacy issues.

[42] Some business enterprises may have established rules for risk identification, analysis, and evaluation regarding projects of new businesses and business development and the functions of the Organization for Privacy Protection built into appropriate departments or divisions in the course of the assessment process.

relationships with experts in privacy issues (scholars, consultants, attorneys, consumer organizations, etc.) and consult with them when necessary.

In addition, when addressing a privacy issue that has been identified, it is required that privacy risk management should be implemented in coordination with the business divisions to realize the objective of the target business operation in the best way possible. In some cases, multiple sided countermeasures, including the proposal of more positive improvement ideas, should be reviewed, rather than simply reacting to avoid risks.[43] In such cases, it is also necessary to check into matters from the viewpoint of regulatory laws and compliance and of the system and information security, in addition to the viewpoint of the business scheme. Additionally, reviews should be conducted with attention to acceptability by users and consumers of services.

In these reviews, it is important to coordinate not only with new business and new technology development divisions, but also those covering legal affairs, information technology systems, information security, compliance, publicity, customer service, corporate planning, as well as those divisions responsible for matters related to human rights, ESG, and sustainability[44], which are relevant when necessary. It is desirable to establish the system so that the necessary members can be summoned flexibly and quickly (for example, by appointing in advance the members in charge in each department).[45]

In actual business operations, the initial response in the event of a privacy issue, as well as the follow-up actions including damage relief, cause analysis

---

[43] Refer to the privacy by design (PbD) philosophy and "positive-sum, not zero-sum" concept in the 7 Foundational Principles (See Chapter 7 "Reference: Privacy by Design").

[44] Taking appropriate action, including the development of internal schemes and systems, to prevent the occurrence of privacy issues, meets the demands of society for corporate social responsibility, as well as the Guiding Principles on Business and Human Rights., as shown in the text of Section 2.3, Importance of Corporate Privacy Governance, footnote 15 and footnote 16.

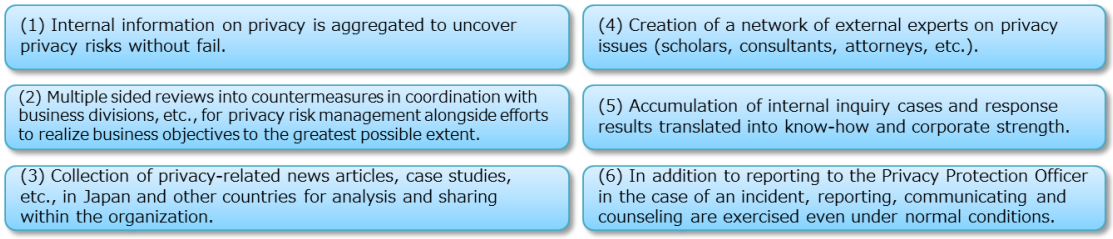
[45] In the past, the study into privacy issues in conducting business focused chiefly from the viewpoint of compliance with the APPI. For this reason, study within the scope of compliance with the Act has been conducted by the legal affairs division in many cases. On the other hand, the scope of attention required from the viewpoint of privacy protection undergoes change and expansion with technological innovation and the rise in consumer awareness toward privacy. It is necessary to create an organization for privacy protection that enables multiple sided study into privacy issues. Although what is appropriate as an Organization for Privacy Protection may differ by the line of business, data handled, etc., there are cases of expanding technological manpower and of organizations consisting chiefly of information security personnel.

and redress, requires information aggregating and analysis in collaboration with the business division(s) and reporting to the Officer Responsible for Privacy Protection to obtain instructions.

It also is necessary to keep information on research into the privacy issue as a history and refer to it when necessary. It is important to routinely collect information on inquiries and issues associated with privacy within the organization and to report them to the Officer Responsible for Privacy Protection, as well as to share them throughout the enterprise.

For the Organization for Privacy Protection to function, personnel capable of compiling the content of the multiple sided reviews and of coordinating interaction among multiple business divisions are essential. In addition to the appropriate assignment of such personnel, manpower training needs to be conducted systematically from the long- and medium-term perspective, in the view that privacy-related activity requires a high level of expertise.

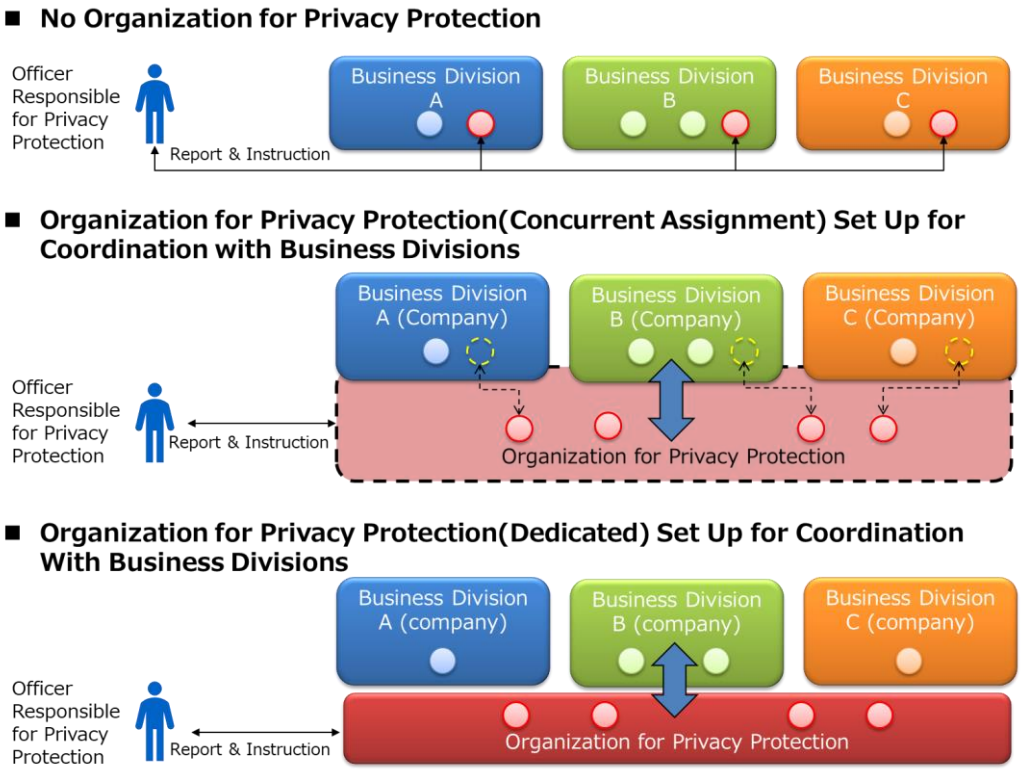
**Figure 7. The Role of the Organization for Privacy Protection**




The privacy protection organization differs in form, depending on the business enterprise. It is important to examine the organizational form alongside the available resources.

Determining which business division the Organization for Privacy Protection will actually be linked to in the structure of the business enterprise is expected to be variable by the business enterprise, due to a variety of factors such as business scale, governance system, type of information handled, location of the organization, etc. (See the example below.) The key is that the organization, regardless of its form or position, must be capable of the swift identification of privacy risks and actual issues that will be caused by the enterprise and report to the Officer Responsible for Privacy Protection to receive instructions.

Figure 8. Example of the Position of the Organization for Privacy Protection Within the Corporate Structure




4.1.3. The Role of The Business Division

The business division needs to check into whether there is likelihood of privacy issues related to its own products and services as well as in the data handled within the division. Awareness and voluntary action by the business division are extremely important. The division should not conduct such checks independently but in close and frequent coordination with the Organization for Privacy Protection, to promote privacy risk management (to identify, analyze, evaluate, and treat privacy risks). If the division is in contact with consumers, it should have adequate awareness that it holds an important position in establishing ties of trust with consumers and to pay due attention to consumer acceptance, etc.

It is important to work in close coordination with its customer satisfaction division, etc., and build a system for regularly gathering a wide range of consumer opinions, as an organization responsible for service provision and operations. For example, attention should be paid to reviews on products and services, etc., (such as reviews in the application store) and information

transmission by consumers in social media, to be able to assess the consumer response swiftly. It also is important to share information on a daily basis so that the business division can make a swift response and coordinate with the Organization for Privacy Protection when an issue occurs.

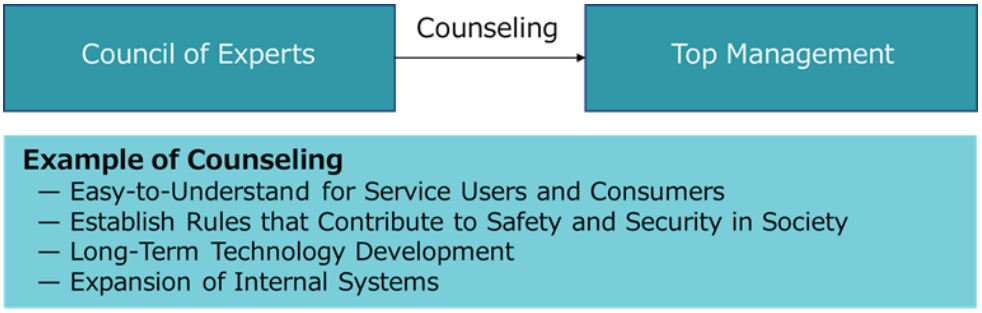
#### 4.1.4. The Role of Third-Party Organizations, Such as the Internal Audit Division and Advisory Boards

If privacy risk management can be monitored and assessed properly from an independent standpoint, activities within the enterprise can be implemented exhaustively. This will also serve as a basis for gaining outside trust regarding the enterprise's activities. An example of this would be the creation of a scheme for internal audit independent of the business execution division, risk management division, etc. In addition, establishing a privacy protection advisory board, advisory committee, etc., and being monitored and assessed from external experts should be one of the options for business enterprises. Experts could be, for example, scholars with extensive knowledge of privacy issues, consultants, attorneys, consumer organizations, etc.

The establishment of an advisory board, etc., will enable the business enterprise to obtain objective and honest opinions prior to a service release or opinions about an appropriate response when an issue occurs in advance. Development of a system or mechanism of feeding back the specialized and objective opinions of experts to business leaders and the employees can also raise awareness of privacy issues and privacy risks throughout the organization.

### Example: Installation of an Outside Expert Council at Safie

Safie Inc. has taken action to maintain the soundness of its image platform handling massive data by setting up a council of outside experts that convenes several times a year. The council consists of legal scholars, attorneys, outside directors, business partners, etc. The council discussed on the establishment of "Safie Data Charter" and conducts continuous deliberations regarding necessary actions to fulfill its responsibilities as a platformer amid changing social conditions. Based on advice received from the council, it also engages in technology development, continual improvement of rules, etc., and awareness promotion among user businesses regarding attention to privacy in data (e.g., Information dissemination on webpages for businesses that installed cameras).




Source: Internal Reference Materials

### Example: Installation of the NEC Digital Trust Advisory Council

NEC Corporation has set up the Digital Trust Advisory Council to enable them to receive a wide range of opinions from external experts so that they can utilize them in management decision-making and policy planning. The Council convenes twice a year. The Council consists of five members who include a legal scholar, lawyer, representative of a consumer organization, and a representative of an NPO in the fields of sustainability, human rights, etc. to obtain not only their specialized knowledge but views from the consumer standpoint as well.

Based on domestic and foreign developments related to privacy, the Council discusses future developments regarding laws, regulations, social acceptance and initiatives that require further reinforcement.

Source: https://www.nec.com/en/global/csr/society/ai.html

## 4.2. Establishment and Dissemination of Management Rules

To make the system described in 4.1 function substantially, privacy risks are required to be assessed and reviewed appropriately by the Officer Responsible for Privacy Protection and the Organization for Privacy Protection, prior to the development and provision of products/services or technology. It is important that the rules for exhaustive implementation established within the organization under the responsibility of the Officer Responsible for Privacy Protection.

For example, rules should be established on measures for privacy protection and from the viewpoint of "who" is to identify, analyze, and evaluate privacy risks and "when."[46] However, it is necessary to ensure the understanding and entrenchment of the philosophy and principles, so as not to invite a stereotypical and uniform response, as well as to conduct continual review and revision of the content.

The Officer Responsible for Privacy Protection and the Organization for Privacy Protection needs to disseminate and entrench the rules throughout business enterprise.

## 4.3. Cultivation of Corporate Culture of Privacy

For a system of privacy governance and its operations put in practice to function appropriately, business leaders need to disseminate the explicitly stated corporate policies throughout the organization and cultivate a corporate culture[47] that enables a proper privacy risk response. Rather than raising awareness of compliance as a general idea, it is important for each employee to be aware of privacy-related issues as one's own — both as an individual person and as a consumer. It is best that such an employee gains a deeper understanding of consumer awareness and anxieties regarding personal data utilization by business enterprises, as well as the information and activities, etc., required, and behaves proactively and with careful attention to society. For this corporate culture to take root, activities are required to–be conducted continuously at various times in the business practice. It is also important that business leaders and the Officer

[46] See Section 5.4 "Privacy Impact Assessment (PIA)" for examples of by "who" and "when" risk identification, analysis, and evaluation are done, etc.
[47] Corporate culture refers to the aggregate of values and behavioral patterns shared by employees.

Responsible for Privacy Protection constantly communicate the business enterprise's privacy governance as stated explicitly, with attention to which values it is going to offer through personal data utilization, as well as promoting the acquisition of basic privacy-related knowledge. These activities serve as the foundation of expert human resources development within the enterprise.

Due to the continuous changes regarding privacy, training adapted to the latest developments and business content is necessary. The following are examples of activities related to the cultivation of a privacy-focused corporate culture.

- Training support during new employee assignment and job rotation.
- Reference to the staff on privacy issues through required reading (booklets, etc.) for employees, etc.
- Regular e-learning and training programs.
- Coordination with seminars organized by the human resources division.
- Distribution of handbooks, etc., linked to corporate policy on privacy issues.
- Awareness promotion, such as internal communication of the activities of the Officer Responsible for Privacy Protection.
- Organizations subject to regular job rotations are added to the Organization for Privacy Protection.
- Training is implemented intensively to business divisions and departments handling personal data.

## 4.4. Communication with Consumers

Continuous communication with consumers is necessary in privacy governance. It is also necessary for the business enterprise to understand consumer awareness and anxieties toward personal data utilization, as well as the information, activities, etc. required, and constantly assess changes taking place in social acceptance. At the same time, it is important for the business enterprise to give careful explanations to consumers actively, clearly, and carefully as to how it is engaged in creating innovation and managing privacy risks and what actions it will take in the event an issue occurs.

Fulfilling accountability toward consumers is essential in building trust with consumers.

### 4.4.1. Announcement and Communication of Corporate Activities

It is important for the business enterprise to organize and announce publicly its stance towards privacy protection and how it identifies, evaluates, and controls privacy risks.

For instance, an effective way is to publish information on matters that are of special concern to consumers both actively and clearly; for example, in a transparency report.[48] Since new privacy risks have emerged with greater sophistication in data utilization, the communication of information on the enterprise's activities on a regular basis, to untangle consumer concerns, will enable consumers to use their services with a sense of security.

Also, there are a growing number of business enterprises that announce the policies and other details of their new projects utilizing personal data prior to the execution of such projects. There are cases of trial project startups after the acceptance, study and application of comments gathered from consumers and reviews conducted based on the findings before the launch of a project. This approach has become accepted as a form of communication to build trust with consumers and society.

### 4.4.2. Continual Communication with Consumers

In addition to periodical reports, when a function is added or updated or when the terms of use are revised, etc., explaining the improvements that have been made regarding their service and response to privacy risks, both swiftly and clearly via their website, etc., provides information quickly to consumers and gains consumer trust regarding the service. In information updates, push notifications of update information to users and notifications to users not particularly attentive to privacy settings to consider checking or reviewing these are important. A continual and active approach by the business enterprise to consumers is valuable from the viewpoint of gaining trust.

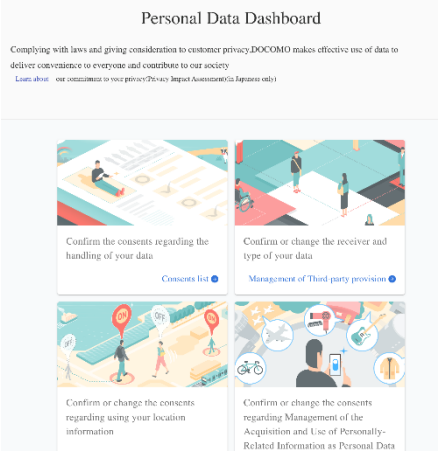
---

[48] A transparency report is a report published periodically by a business enterprise to guarantee the transparency of its data handling to consumers.

Another form of continual communication is notifying consumers about access to customer service and offering them the use of a control panel regarding data handling to help them express their opinions regarding the utilization of their own data.

**Example: NTT DOCOMO Personal Data Dashboard for Customers**

NTT DOCOMO offers its customers features for confirming and changing the receiver and type of their data, and confirming the consents regarding the handling of their data.




Source: https://datadashboard.front.smt.docomo.ne.jp/en

In view of the fact that privacy is subject to change, consumer awareness needs to be identified from various consumer contact points.

In the case of a business enterprise whose business is centered on data analysis collaborates with a business enterprise whose operation is in face-to-face contact with consumers on a daily basis, the former needs to increase its own knowledge of privacy protection by organizing awareness surveys on privacy issues continuously and assessing social acceptability, etc. It is important not only to be satisfied with doing surveys but also to apply the results to the enterprise's own activities.

**Example: Hitachi and Hakuhodo Opinion Surveys Regarding Consumer Information**

Hitachi Ltd. and Hakuhodo Inc. are conducting opinion surveys on a continual basis for the quantitative assessment of changes in people's awareness.

**Activities at Hitachi**

- Hitachi/Hakuhodo opinion surveys on consumer information handled as big data.
  Hitachi and Hakuhodo are conducting opinion surveys on a continual basis for the quantitative assessment of people's awareness about personal data utilization progresses. Surveys were conducted five times - the latest in 2020.
  The third survey in 2016 examined the expectations, concerns, etc., toward IoT and AI representing the latest technological trends. Survey results are used to develop policy and activity on these issues.


Source:
https://www.hitachi.co.jp/products/it/bigdata/bigdata_ai/personaldata_privacy/index.html
Reference: 5th Opinion Survey Regarding Consumer Information Handled as Big Data (Hitachi, 2020)
https://www.hitachi.co.jp/New/cnews/month/2020/12/1222a.html

### 4.4.3. Consumer Communication in Case of a Problem

In the event of an actual privacy problem, the occurrence should be identified swiftly and addressed after assessing the details. As described in 4.1, an organization-wide scheme including the related divisions and the flow of action to address such a situation should be examined and established prior to the release of products or services.

Consumers who sustain real damages from data leakage, etc., should receive an apology and be clearly informed of the enterprise's knowledge of the scope of the event that occurred, the cause, and the measures that have been implemented to deal with the problem. In particular, when there are consumers who are likely to sustain secondary damages, all means should be taken to notify consumers individually if possible or through a press release if not so that the customers can take measures to avert and mitigate secondary damages (change of PIN, etc.). Due to the possibility that damages can be magnified by provision of this information, depending on the nature of

the problem this information should be provided through consultation with security experts.

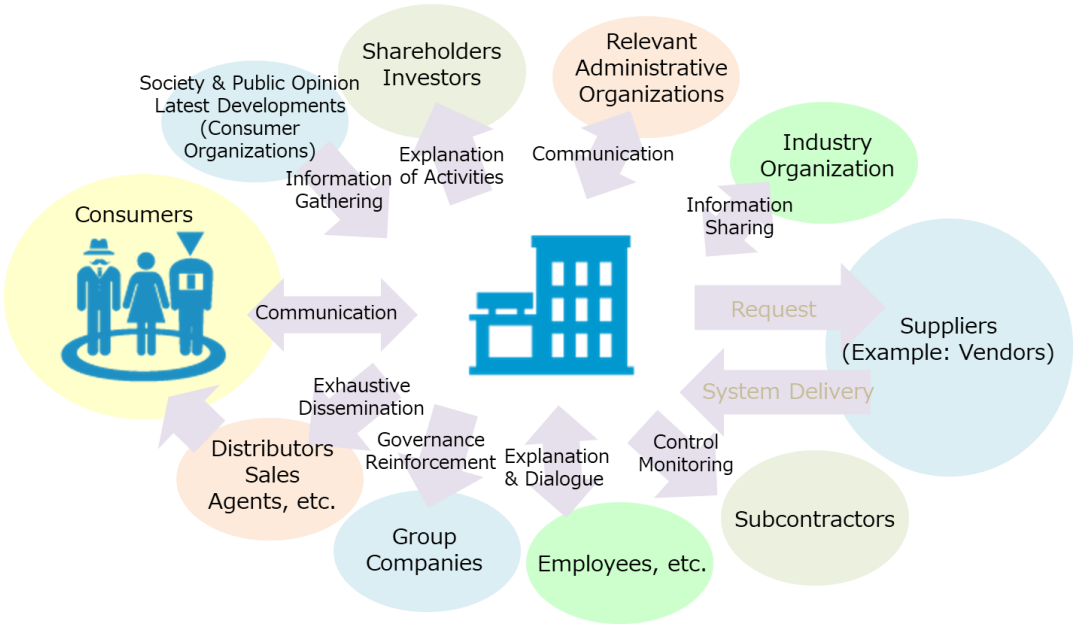
## 4.5. Communication with Other Stakeholders

In privacy governance, continual communication is required to be maintained with stakeholders of the business enterprise— actively giving explanations on how the business enterprise is engaging initiatively in innovation creation and in privacy risk management — in order to gain their trust.

### 4.5.1. Response to Stakeholders

Privacy-related activities require the development of relations not only with consumers but with each stakeholder.

**Figure 9. Communication with Stakeholders**



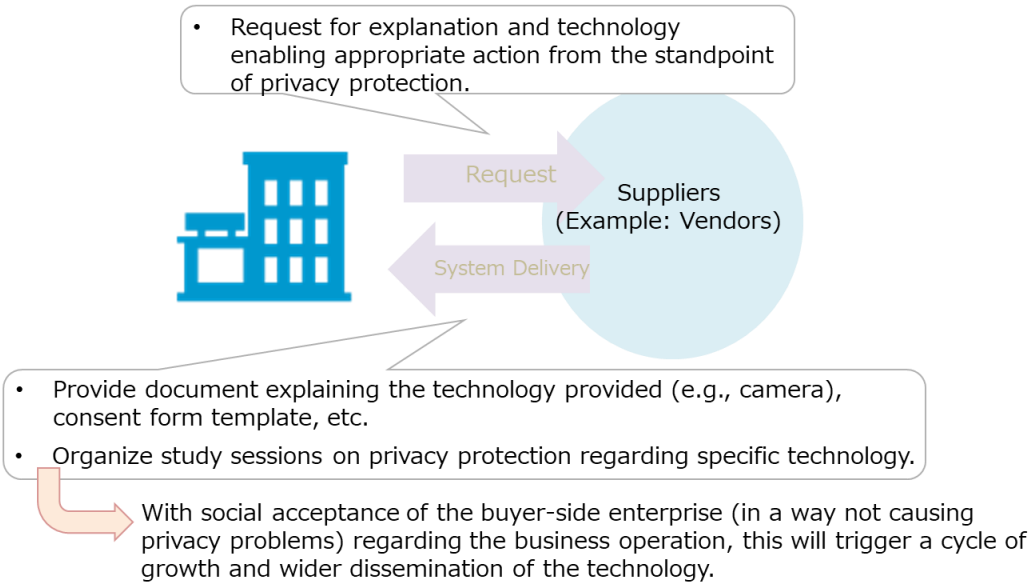
(1) Business Partners (Suppliers and Subcontractors)

Due to the need of a business enterprise to collaborate with multiple business enterprises, such as business partners, in executing their business operations, if actions to address privacy risks by the business enterprise and other business partners are not appropriate, all of the relevant business enterprises (including one's own business enterprise) and the entire business project may incur in the loss of consumer trust.

Since new privacy risks may emerge in areas where technological innovation takes place rapidly, close communication with vendors and other system-related suppliers is especially important, assuming that consumers' concerns about privacy are subject to change. Concerns regarding consumer privacy risks should be examined continuously, and the relevant enterprises should check into systems as to whether a preparatory response is possible and appropriate action should be taken.

The buyer-side enterprise should require the supplier (vendor, etc.) to provide technology and an explanation to enable proper actions related to privacy protection. The supplier should give a thorough explanation and enable the buyer to operate the system designed to address privacy issues by providing explanatory documents regarding the technology provided, guidelines relating to privacy in technology use, a template consent form, etc. It is also effective to organize study sessions for the buyer-side enterprise to deepen their understanding. This will result in a positive growth cycle of social acceptance of the products and services of the buyer-side enterprise free of privacy problems, leading to further dissemination of the supplier's technology.

**Figure 10. Example of Communication with Suppliers**




Furthermore, in outsourcing a business operation to another business enterprise, the outsourcing enterprise will also be responsible for any problem caused by the operation. For this reason, subcontractors should be selected from the viewpoint of privacy protection by examining their ability to address such matters properly. The outsourcing enterprise should require the subcontractor to explain its organization, technology, etc. relating to privacy protection activity. The subcontractor needs to cooperate with the outsourcing enterprise to boost its privacy-related activities. In the event of a privacy issue, the outsourcing enterprise must take action with sincerity toward its customers and consumers.

(2) Group Companies, etc.

Even in business operations conducted chiefly by a subsidiary, etc., in a corporate group, a privacy problem may result in the loss of trust and brand reputation for the entire group. For this reason, attention will be required regarding privacy risk handling. The nature of the Organization for Privacy Protection for the entire group and the role and responsibilities of the holding company requires study, as well.

If there are business sites overseas, attention should be directed to the response in each country, due to differences in privacy-related activities by country.[49]

### (3) Investors and Shareholders

There is also a tendency among investors to perceive reinforcement of the risk management organization not as cost but as advance investment, shifting away from the viewpoint of the impact on corporate performance and social responsibility.[50] There will be an increasing demand for business enterprises to give a clear explanation of their action on privacy risks to shareholders and investors, as well. The production and release of a transparency report and pertinent information in an integrated report or a sustainability report are ways to explain with a high level of transparency. It is important to choose the option appropriate to the scale, resources, etc., of the business enterprise.

### (4) Relevant Administrative Organizations

A routine check of the liaison offices representing the administrative organizations, such as the Personal Information Protection Commission(PPC), working on personal data utilization and privacy issues and counseling with such an office prior to the startup of a business project, is important.[51] In addition, compliance with the laws specific to the business or industry and the guidelines established by the relevant administrative government organizations are required, along with proper implementation based on the special characteristics of the industry, in communications with such organizations, may be necessary, depending on the industry.

---

[49] See Chapter 6 "Reference: Methods for Collecting Information on Foreign Laws and Regulations, etc." for how to collect information on laws and regulations in other countries.
[50] Momentum is growing to direct attention to the interests of all stakeholders can be seen in "stakeholder capitalism" discussed in the Davos Manifesto and the BRT Statement of the Business Roundtable of the United States.
[51] As part of the drive to foster the protection of personal information by business enterprises and the appropriate and effective utilization of such information, the PPC Business Support Desk, set up by the PPC, accepts inquiries regarding matters requiring attention under the APPI for new business models with new technologies.

(5) Industry Organizations

Depending on the industry, industry associations or accredited personal information protection organizations are in place, and conduct research/surveys, publicity and public relations activities, announcements of opinions and liaisons/recommendations submitted to relevant administrative organizations, to aim for the sound development of the industry and to build understanding among consumers. The occurrence of a privacy issue by a competitor in the same field of technology is likely to lead to a loss of consumer trust for similar products and services, etc., of one's own business. Therefore, it is necessary to participate actively in information sharing regarding privacy issues and privacy risks through industry organizations, etc., and to provide and obtain information actively. In addition, it is necessary to improve the environment to enable the effective use of the information received.[52]

(6) Employees, Etc.

Because of the need of a business enterprise to handle the privacy-related information of employees, attention to employee privacy is required, as well. On the other hand, there are situations in which employee privacy must be restricted, due to demand from security and other needs in business operation. Furthermore, the management of employee-related information is accompanied by the risk of information leakage. Therefore, employees should be regarded as a target for communication and for conducting action such as dialogue with employees, an announcement or explanation through the representatives for the employees.[53] This applies not only to the employees of the business enterprise but also to job candidates, retirees, employees of the suppliers, etc.

---

[52] For example, the Japan Electronics and Information Technology Industries Association issued its Guideline on Smart Home IoT Data Privacy in March 2023 to provide basic guidance in handling IoT data that is the data on everyday living in the smart home. The Guideline also illustrates the minimum in data handling to be achieved by relevant parties, when collecting and utilizing such data with attention to protection of personal information and privacy.

[53] There were incidents of improper data analysis and utilization in the recruitment of new employees (new university graduates) in 2019. Since the same structure applies to employee monitoring, attention should be paid to the fact that the responsibility lies not only in the provider of data analysis. The business enterprise utilizing the information also will be held liable for the same or greater responsibility.

### 4.5.2. Information Collection on Privacy Issues

Due to the continual changes taking place in the scope of privacy, it is important not only to conduct the consumer awareness surveys mentioned earlier but also to obtain on an ongoing basis information on developments in legal schemes in Japan and other countries, exchange information with industry organizations, and acquire information on the latest developments in society and in public opinion.

In particular, the website of PPC offers relevant information, including that on the APPI, related guidelines, Q&A, etc. The personal information protection-related website of the Ministry of Economy, Trade and Industry offers information such as study results on personal data, etc., that the Ministry has conducted in the past.[54]

It is also beneficial to collect information from privacy and security experts on the enterprise's advisory board, attorneys with extensive knowledge on privacy, etc.

### 4.5.3. Other Activities

If the assessment of privacy risks and studies into countermeasures are difficult for a single business enterprise, or when actions as an industry or an industry-wide response are necessary, these activities can be organized chiefly through consortia managed by industry associations, the Japanese government, or jointly between the government and private sectors, to summon experts to study into matters requiring attention and the appropriate response and to publish the findings.[55]

[54] Privacy Governance page, Ministry of Economy, Trade and Industry website: https://www.meti.go.jp/policy/it_policy/privacy/privacy.html

[55] An example is the review and publication of "Guidebook for Utilization of Camera Images" (IoT Acceleration Consortium, Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications).

# 5. Reference: Approach to Responding Privacy Risks

In handling privacy issues, a risk-based approach should be adopted in identifying risks and implementing measures against risks with agility. The following shows the approach and information to serve as reference in privacy risk management (risk identification, analysis, evaluation, and treatment). It must be noted that the information here is not presented systematically strictly for reference. The information is to be used as a reference when a business enterprise is to implement privacy risk management.

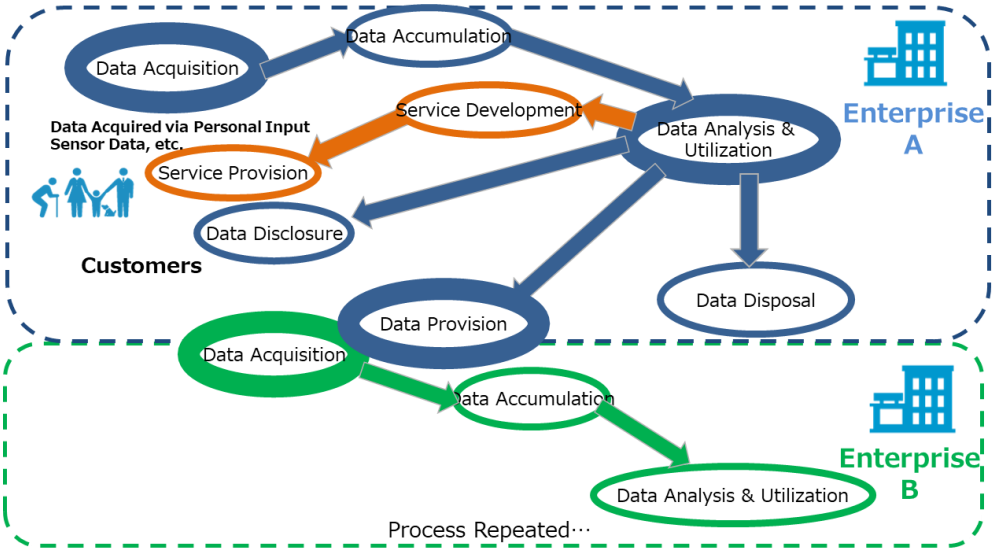
## 5.1. Interested Parties, Identification of Personal Data to be Handled, and Organizing the Lifecycle

In identifying privacy risks, the lifecycle of personal data used in the specific business operation is required to be organized. The key points that require organization are the following

- ✓ Identifying the interested parties for the specific business operation (consumers and business partners (suppliers, subcontractors, etc.).
- ✓ Identifying the personal data to be handled in the specific business operation (personal data to be identified consists not only of data acquired directly but also data that can be inferred through third-party purchasing and profiling).

The figure below illustrates the example of a lifecycle from data acquisition to data re-provision and disposal. It is also necessary to organize what part will be outsourced, whether there is an outsourcing service with whom data will be used jointly, etc., along with organization of the relationships with relevant business partners to match with the check into the data lifecycle. This scheme involving outsourcing service providers should be decided upon at an early stage to define the obligations these providers need to fulfill in compliance with laws and regulations.

Figure 11. Example of Personal Data Lifecycle




In implementing visibility of the personal data lifecycle, some segments may become easy for consumers to identify and some may not. In particular, the utilization of personal data acquired via IoT devices such as cameras and sensors and data obtained by inference via profiling, etc., is likely to cause privacy problems. For this reason, it is necessary to give a careful explanation to consumers of their own privacy risk identification, analysis, evaluation, and treatment, and of how personal data will be utilized, along with their objectives.

Furthermore, matters related to the role of actors in personal identifiable information (PII), the scenario of the PII exchange among the actors and identification of PII (in which situations the information will be determined as PII) can be found in 4., Basic Elements of the Privacy Framework of ISO/IEC 29100:2011 Privacy Framework (JIS X 9250:2017 Information Technology — Security Techniques — Privacy Framework) for reference.

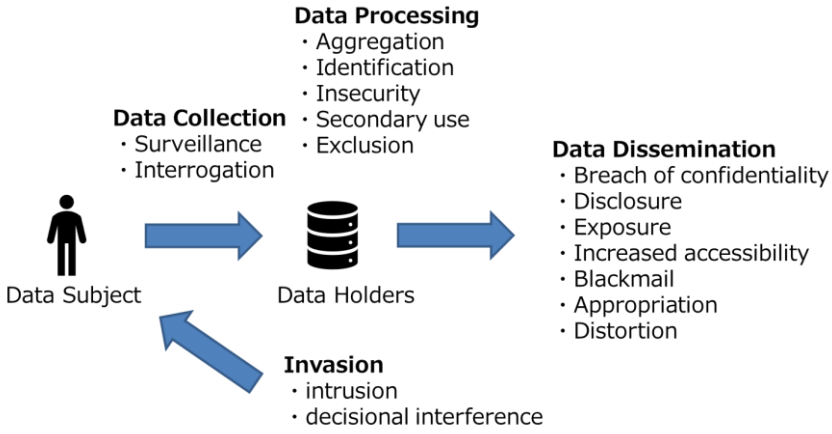
## 5.2. Identifying Privacy Issues

Privacy issues that are likely to emerge in the personal data lifecycle are identified for study into how such issues are to be treated.

Although strictly a sample, the following illustrates which privacy issues are likely to emerge in each stage of the personal data lifecycle. It is important

that, in the course of study into the system requirements and administration of the target business operation, privacy issues are identified with attention to the distinctive features of the operation and to the information obtained in the study and with a check against business leaders ' stance on privacy governance, etc., that has been announced explicitly.

**Figure 12. Classification of Activities That Create Privacy Issues**




Source: Figure modified by the Secretariat based on "A Taxonomy of Privacy" (Daniel J. Solove, 2006)

## Figure 13. Examples of Privacy Issues

| | | |
|---|---|---|
| Data Collection | Surveillance | Likelihood of anxiety, discomfort and other negative sentiments in the individual, caused by continual monitoring. |
| | Interrogation | Application of coercion on the individual to pry for information and cause anxiety, with questions delving deep into the person's privacy. |
| Data Processing[56] | Aggregation | The possibility of betraying the expectations of an individual through the collection of fragments of information on the person to reveal new evidence that had been unimaginable to the person. |
| | Identification | Through connection of all possible data to individual persons, harmful information may be connected to the person, possibly raising anxiety and dissatisfaction. |
| | Insecurity | Failure to ensure appropriate protection of personal data may go against the interests of an individual. |
| | Secondary Use | Use of data for purposes other than the initial objective and without consent of the individual may be a betrayal to the person. |
| | Exclusion | By denying the right of the individual to data disclosure and revision, etc., the person may be deprived of control over important decision-making. |
| Data Dissemination | Breach of Confidentiality | Disclosure of data of an individual obtained through a relationship based on trust is likely to destroy the relationship (regardless of the nature of the data exposed). The individual may feel betrayed. |
| | Disclosure | Disclosure of data of an individual may cause further privacy issues for the recipient of the data for secondary use. |
| | Exposure | Exposure of the various aspects of life to others may result in grievous shame and obstruction of the person's ability to participate in society. |
| | Increased Accessibility | Increase in the possibility of third-party access to personal data may lead to an increase in disclosure risk. |
| | Blackmail | The likelihood of creating a strong power relationship, setting provisions such as the exposure of personal data and disclosure to third parties, resulting in domination and control of the individual. |
| | Appropriation | Unauthorized appropriation of the identity or personality (e.g., name, image, etc., but not necessarily limited to these) of an individual person for the purposes of another party, in order to deprive the individual's control over how to express oneself in society and interfere with the person's freedom in exercising their personal authorship. |
| | Distortion | Through control of how an individual is perceived and judged by others and the display of information that may invite distortion, there is likelihood of inviting disgrace, stigma, and threat to the reputation of the person. Also, the likelihood of distortion of an individual's reputation and personality that are essential to establishing the person's own identity and to the person's capability to engage in |

[56] In a society founded on AI, it is likely to identify from inference an individual's political stance, financial status, interests, and hobbies, etc., with a high level of accuracy from data related to the person's behaviors, etc. Through the distribution or utilization of data in a way not desired by the individual, problems may occur, such as the infringement of personal freedom, dignity, and equality. These problems will be deemed likely as privacy issues resulting from "Aggregation" and "Identification". (The basic principle in assuring privacy is also found in Social Principles on Human-centric AI, (Council for Science, Technology and Innovation, 2019. Additionally, the Final Recommendations on Profiling (Personal Data +α Study Group, 2022) lists the important points of note in the analysis and forecast of preferences and interests, capabilities, credibility, intelligence, behavior, etc., of specific individuals (profiling) utilizing personal data and algorithms, considering their risks about the relations between effective data utilization and privacy rights, fundamental principles of equality or democracy.)

| | | |
|---|---|---|
| | | communal living. This may lead to the arbitrary and unsuitable distortion of social relationships. |
| Invasion | Intrusion | The approach to an individual in inordinate frequency (email, telephone call, etc.) that results in obstruction of the person's everyday routine, raising their sense of insecurity and discomfort. |
| | Decisional Interference | In the case of use of AI in important decision-making in an individual's life, the decision-making method may be unclear and result in a chilling effect on the person. |

Source: Figure compiled by the Secretariat based on "A Taxonomy of Privacy," (Daniel J. Solove, 2006).

## 5.3. Identifying Privacy Risks

In identifying the risks that emerge in a business enterprise's personal data lifecycle, caused by privacy issues and affecting individuals and society (privacy risks), frameworks, etc., may serve as a reference.

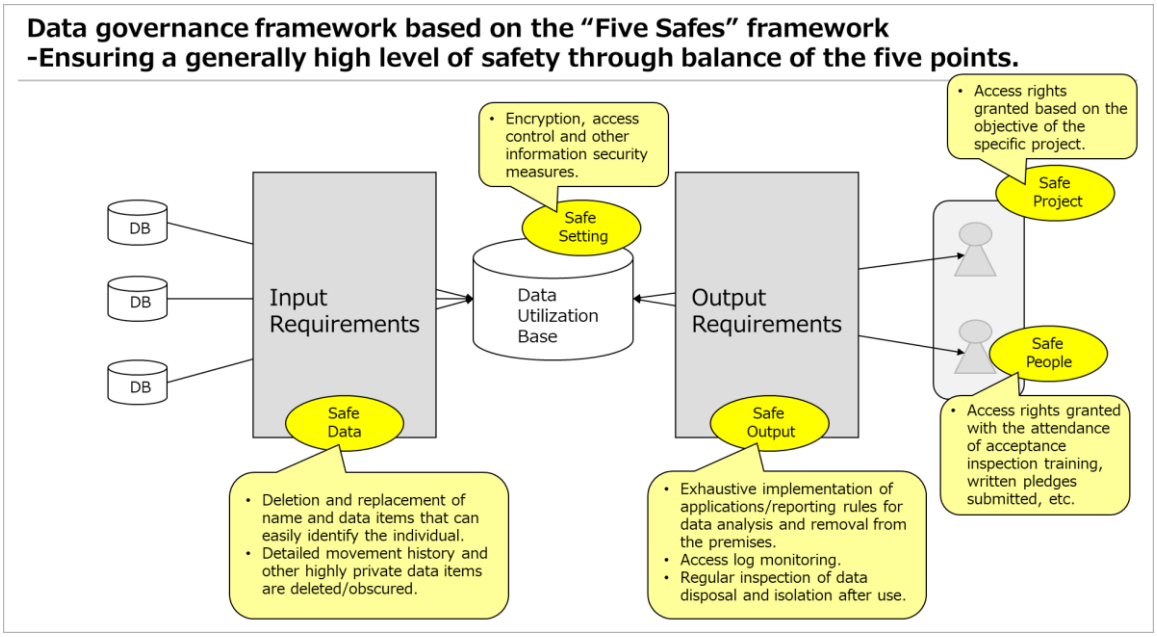
An example is the Five Safes model that has been implemented since 2003 by the UK Office for National Statistics (ONS) as a method for handling data safely while assuring data availability, to regulate research employing confidential information. The Five Safes model has been used widely, not only in the European Union but also in other regions and countries as a set of rules for the utilization of individual data and statistics as well as for safety in data utilization. It also serves as a reference in the study of privacy issues and their control methods.

**Figure 14. Reference: Summary of the "Five Safes" Model**

| Item | Description |
|---|---|
| Safe Project | Whether the objective of the data use and handling is appropriate in terms of legal and social norms. |
| Safe People | Whether the researcher is reliable regarding the appropriate use of individual data. |
| Safe Data | Whether there is the risk of confidential information disclosure in the data itself. |
| Safe Setting | Whether the system environment restricts unauthorized use. |
| Safe Output | Whether there is the risk of confidential information disclosure in the analytic results. |

Source: Tanvi Desai, et al. "Five Safes: designing data access for research" (University of the West of England), 2016

Figure 15. Reference: Data Governance Framework Based on the "Five Safes" Model




## 5.4. Privacy Impact Assessment (PIA)

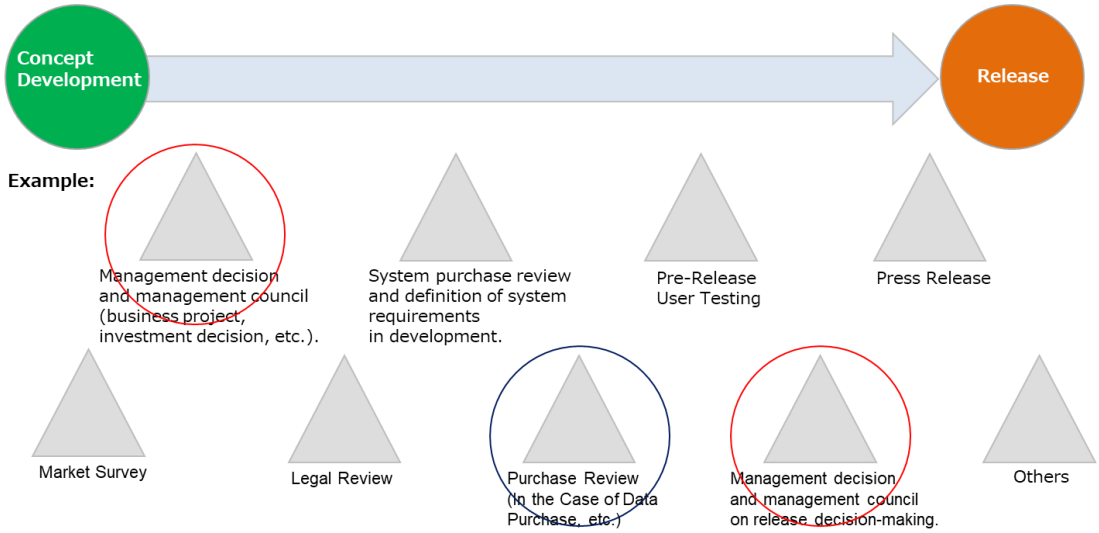
Privacy impact assessment (PIA) is a method of identifying, analyzing, and evaluating risks related to personal information and privacy, and considering how to deal with them.

The important points in identifying, analyzing, evaluating and treating privacy risks are who does that and when. If privacy risk is found to be high immediately prior to a service release, for example, there will be no time to plan control measures. Conversely, if an assessment is conducted too early, it may be difficult to visualize clearly the potential privacy risks.

The figure below shows the steps to be taken by a business division until a product or service release. In a business project likely to involve a high level of privacy risk, identifying, analyzing, and evaluating privacy risk with business leaders may be conducted during an early phase of project review and during release decision-making. Another possibility is identifying, analyzing, and evaluating privacy risk prior to a review into system specifications, to implement control measures and to check at the time of release decision-making whether risks have been reduced. If there are

residual risks, it is also possible to plan post-release handling in advance. If an external service is to be employed or data is to be purchased from an outside source, a privacy risk identification, analysis and evaluation at contract review or at a data purchase review conducted jointly with the legal affairs division and an Organization for Privacy Protection is believed to be effective.

**Figure 16. Example: Steps Leading to Product or Service Release**




Although who identifies, analyzes, and evaluates privacy risks and when may differ by business scale, line of business, content of the personal data to be utilized, etc. It is important to establish the rules appropriately, for example, by classifying the situation of who should evaluate privacy risks and when by a pattern.[57,58]

The information obtained through system operations for a specific period also may be consolidated for the development of a template for the information necessary to evaluate privacy risks and the production of a checklist. However, it is necessary to prevent the checklist and template from

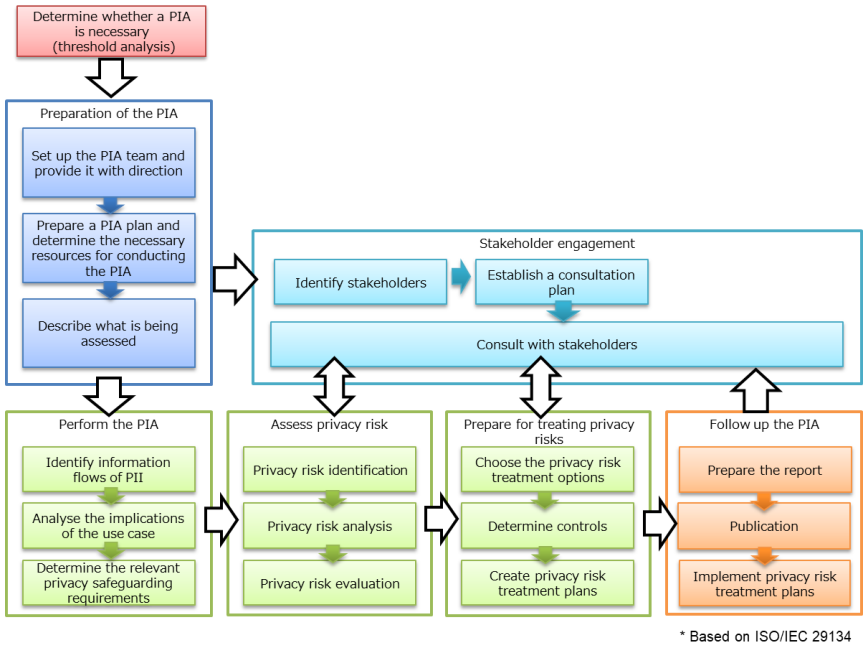
[57] The effective use of the existing systems and workflows for the identification, analysis, and evaluation of security and other risks in the business enterprise, establishment of rules beginning with business divisions that make extensive utilization of personal data, and other ideals may lead to efficient management.

[58] If development takes the agile approach rather than waterfall, it is necessary that the product owner and other interested parties at the worksite are constantly aware of privacy issues when taking action. In addition, it is important that a check is conducted during release decision-making without fail to confirm that risks have been minimized.

creating a uniform, stereotypical response and to cultivate a consistent understanding of the basic principles and rules among the participating members. Maintenance including continual review and revision is necessary, as well.

In the ISO/IEC 29134:2017 Guidelines for Privacy Impact Assessment (JIS X 9251:2021 Information Technology — Security Techniques — Guidelines for Privacy Impact Assessment, there are recommendations regarding the PIA process, PIA reporting structure, etc.[59]

**Figure 17. Reference: The Key Points in ISO/IEC 29134 (JIS X9251)**



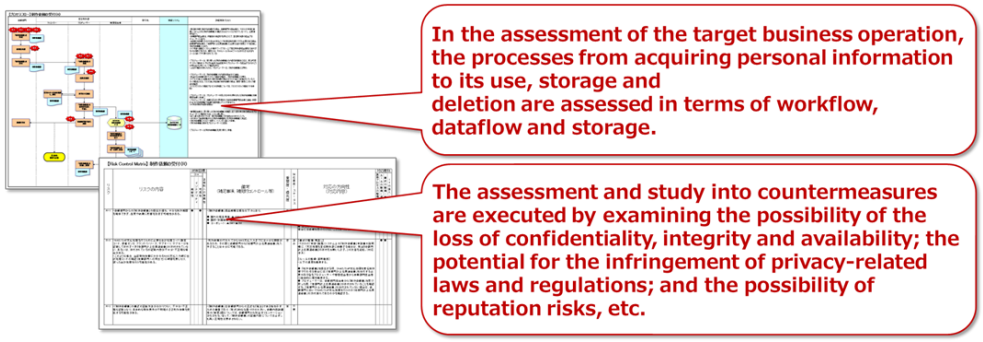

[59] The terms and definitions used in the standard are based on the ISO/IEC29100 privacy framework (JISX9250 Information Technology — Security Techniques — Privacy Framework). Privacy safeguarding requirements are explained in this standard.

ISO/IEC29100 (JISX9250) describes the following as privacy framework. (1) The actors and their roles in processing personally identifiable information (PII); (2) scenarios of interaction among the actors; (3) recognizing PII (in which instances information is assumed to be PII); (4) various factors (laws and regulations, contracts, business and other factors (privacy preferences, etc.) that will affect the set of privacy safeguarding requirements that the organization must take into account in PII processing; (5) matters that must be established by top management of the organization involved in PII processing; and (6) privacy controls. Also, the principles of privacy derived from existing principles developed by countries and international organizations, etc., have been organized into 11 items. The privacy impact assessment (PIA) described in ISO/IEC 29134 (JIS X9251) indicates that this can be integrated into risk management. ISO/IEC 27701 also refers to the standard as an additional guide on the rules for implementing control measures.

In 2021, PPC published Promoting the Implementation of PIA — Significance of PIA and Points to Keep in Mind in the Implementation Procedure to promote voluntary action by business enterprises.[60,61]

**Example: Privacy Impact Assessment (PIA) at Shiseido**

Shiseido Co., Ltd., is engaged in a privacy impact assessment (PIA) as part of the operations of personal information protection. As part of the PIA, personal data handling is visualized by making use of workflow, a detailed description of the operation and a risk control matrix (RCM) approach used in their internal control assessment to promote risk identification and reduction.




Personal data handling is visualized to identify and reduce risks.

Source: Internal Reference Materials

[60] 3-3-2(2) of APPI "Every-Three-Year Review" Outline of the System Reform specifies that "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."

[61] Promoting the Implementation of PIA — Significance of PIA and Points to Keep in Mind in the Implementation Procedure (Summary) (PPC, 2021) https://www.ppc.go.jp/files/pdf/pia_overview.pdf. Promoting the Implementation of PIA — Significance of PIA and Points to Keep in Mind in the Implementation Procedure (PPC, 2021) https://www.ppc.go.jp/files/pdf/pia_promotion.pdf.

## Example: Service Control Meeting at JCB

JCB Co., Ltd., is building and managing a service control meeting (SCM) as a process for assessing risks, not only those related to privacy, and curbing them through early detection of potential risk events in the product/service planning stage.

The SCM administration office and business divisions that handle risks (such as the legal affairs and security divisions) are working with divisions submitting proposals to SCM (such as business divisions) to share, identify and assess risks (numbering approximately several hundred a year). Matters that are to be deliberated and decided upon by the management board are submitted with documents describing the risks that became apparent at SCM and the policies on dealing with these risks, thus enabling top management and officers with decision-making authority to make appropriate decisions in the face of these risks.

At SCM, privacy-related risks are subject to control and assessment as information security risks. In promoting business that utilizes personal data, rules on personal data management have been established as internal rules to provide customers with appropriate privacy protection. The business division submitting a proposal to SCM is able to check their compliance status vis-à-vis compliance with the management rules with the personal data utilization checklist.

【SCM Flow】


【SCM Entry Criteria Example】

| Entry Criteria | Entry Upper Limit (Exclusionary Conditions) |
|---|---|
| New Product/Service Business Development | All Prefectures (No exclusions) |
| Product/Service Termination | All Prefectures (No exclusions) |
| New Credit Card Startup | All Prefectures (No exclusions) |
| Termination of Credit Card Affiliation | Exclude cases not against consumer interest. |
| DM, Sales Campaign, Measures | Exclude cases found to comply with the Act Against Unjustifiable Premiums and Misleading Representations and other laws. |
| Installation/Update of Information System & Devices | When not connected with the Internet and other external networks, excluding installation of hardware units. |
| Subcontracting Business Operation Handling Personal Information | Existing service subcontracting in which there is no change in personal information handling. |

【Rules on personal data management】

| Rules on Personal Data Management | Article |
|---|---|
| Chapter 1 General | 1. Objective |
| | 2. Terminology |
| Chapter 2 Basic Rules on Personal Data Use | 3. Respect for customer sentiment. |
| | 4. Control by the customer. |
| | 5. Clear and easy-to-understand policy. |
| | 6. Measures corresponding to the scale of privacy risk. |
| Chapter 3 Use of Anonymously Processed Information | 7. Use of anonymously processed information. |
| | 8. Production, etc., of anonymously processed information. |
| | 9. Prohibition of identifying behaviors. |
| | 10. Provision of anonymously processed information. |
| | 11. Internal procedures. |

【Personal Data Utilization Checklist】

| # | Personal Data Utilization Checklist | Basic Criteria |
|---|---|---|
| 1 | Respect of Context | Use should not raise anxiety in the customer and be within the foreseeable scope. |
| | | Utilization in a form that matches the customer's expectations and in accordance with the context of the personal data provision by the customer. |
| 2 | Control by the Individual | The customer is guaranteed the opportunity to control one's own data (i.e., the opportunity to intervene in how it is used). |
| | | Opt-in and opt-out from services used appropriately. |
| 3 | Clear and Easy-to-Understand Policy | The customer is informed very clearly as to what data will be used and how. |
| 4 | Measures Corresponding to the Scale of Privacy Risk | Measures to be implemented, vis-à-vis the privacy nature of each data type and the level of risk in the form of data utilization, based on an advanced assessment of their impact on privacy. |

Source: Internal Reference Materials

## 6. Reference: Information Collecting Methods in Relation to Foreign Laws and Regulations, etc.

With the dramatic speed of technological innovation, differences in perception of privacy issues depending on the individual, and changes taking place in social acceptance depending on context and the passage of time, business enterprises need to collect relevant information (on market trends, technologies, regulations, etc.) continuously under the initiative of an Organization for Privacy Protection, etc.

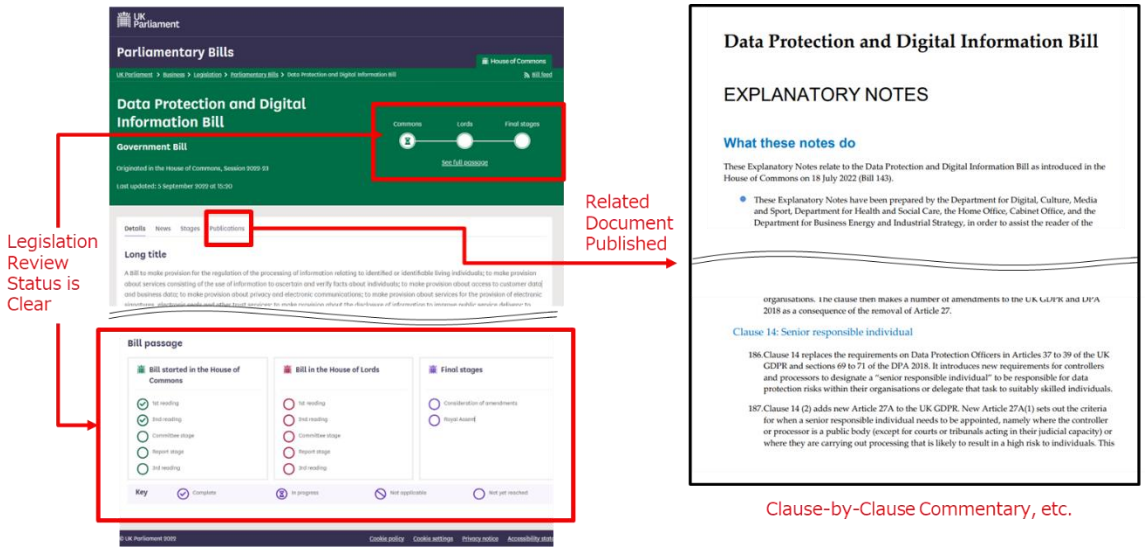
When business enterprises collect information related to foreign laws and regulations, etc., information on the nations researched by the Personal Information Protection Commission (PPC) is available on the PPC website[62]. Additionally, the legislation database of the target country and websites of the administrative agencies relating to the law are useful. The websites of the courts of law in the target country also may be examined as part of a survey of data for possible application if court precedents make up part of important rules.

For example, the website of the UK Information Commissioner's Office (ICO),[63] the regulatory authority in the country, offers information on enforcement actions by the ICO, as well as a data protection guide for businesses enterprises, etc. Regarding British laws, the website of the National Archives (United Kingdom)[64] offers a clause-by-clause explanation. In the UK, Parliament exercises legislative power. When a bill passes the House of Lords and the House of Commons and is ratified by the King, it becomes law.[65] In the Parliamentary Bills pages[66] of the UK Parliament website, a page is created for the law to offer a summary of the bill, the governing agency in charge, the bill, the progress status in bill deliberation, news, related documents (including Explanatory Notes on the bill), and other information.

---

[62] Surveys of Foreign Systems for the Protection of Personal Information, PPC website: https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#gaikoku
[63] UK Information Commissioner's Office (ICO) website: https://ico.org.uk/
[64] The National Archives (United Kingdom) website: https://www.legislation.gov.uk/
[65] The UK Parliament System (National Diet Library Research and Information — ISSUE BRIEF — 2019.5).
https://dl.ndl.go.jp/view/download/digidepo_11286064_po_1056.pdf?contentNo=1
[66] UK Parliament website: Parliamentary Bills: https://bills.parliament.uk/

Figure 18. Legislation-Related Information Service of the UK Parliament




Source: Data Protection and Digital Information Bill page, UK Parliament website (https://bills.parliament.uk/bills/3322)
Source: Data Protection and Digital Information Bill EXPLANATORY NOTES (https://publications.parliament.uk/pa/bills/cbill/58-03/0143/en/220143en.pdf)

Since the United States is a federation of 50 states, information on U.S. federal laws can be found on the website for the House of Representatives' Office of the Law Revision Counsel (the United States Code).[67] The website of the Federal Trade Commission (FTC) overseeing consumer privacy in the U.S.[68] offers related information, as well. The U.S. Congress holds legislative power. Bills that have passed the upper and lower houses become law upon signature by the President of the United States.[69] Bills slated to become federal law, the progress status on deliberations, and other information can be found on the official website for U.S. federal laws (Congress.gov).[70] In the U.S., there are cases of state laws providing comprehensive protection of personal information, such as the California Consumer Protection Act and the California Privacy Rights Act that amended the CCPA. For this reason,

[67] U.S. Office of the Law Revision Counsel (The United States Code) website: http://uscode.house.gov/
[68] Federal Trade Commission (FTC) website: https://www.ftc.gov/
[69] U.S. Congress system (National Diet Library Research and Information — ISSUE BRIEF — 2019.3). https://dl.ndl.go.jp/view/download/digidepo_11247815_po_1045.pdf?contentNo=1
[70] Official website on U.S. federal laws (Congress.gov): https://www.congress.gov/

it is also necessary to examine information released by state authorities regulating data protection.

In addition to information-collecting from data protection organizations, national regulatory authorities on law, governing bodies, etc., of each country (state), there are also databases on privacy-related laws and related news made available with charge by private service providers. In addition, law firms and others offer websites called trackers that offer information on the state of compliance of each nation (whether a law has been passed, whether a bill is still in draft (or bill) stage, whether there is a draft at all, etc.) *vis-à-vis* rules such as the General Data Protection Regulation (GDPR) adopted by European Union, with which each nation is required to comply. Although trackers offer an information service for free in many cases, attention is required as to whether the information is the latest by checking the date of the most recent website update.

When handling the personal data of consumers, etc., on a global scale, adequate attention to the statutory laws and regulations in other countries is required to ensure privacy protection. When comprehensive and general data collecting is necessary, inquiries with law firms in the target countries should be considered, after confirming the qualifications and expertise of such firms, in addition to the methods mentioned in this Chapter.

# 7. Reference: Privacy by Design

The concept of Privacy by Design (PbD) is one of the global standards that offer an approach to basic privacy protection. Rather than dealing with privacy problems in business or in the organization with stop-gap measures, this approach calls for the integration of a privacy protection mechanism in advance into the business model, technology, or initial stage of organization development. It can be summarized into the following five key points.

1. Interest in privacy and awareness that the problem must be resolved.
2. Application of the principles of Fair Information Practices (FIPs).
3. Early detection and mitigation of privacy issues throughout the information lifecycle at the time of the development of an information technology and a system.
4. The need for the provision of information relating to privacy from instructors and experts.
5. Acceptance and integration of privacy-enhancing technologies (PETs).

The concept also specifies seven foundational principles.

**Figure 19. Privacy by Design: The Seven Foundational Principles (Summary)**

| Principle | Description |
|---|---|
| Proactive/Preventive | Proactive rather than reactive; preventive rather than remedial. The objective is prevention before privacy infringement occurs. Privacy by design is characterized by addressing privacy protection, not passively but with foresight. |
| Privacy as the Default Setting | Privacy protection is to be set as the default. This is also known as privacy by default. The privacy protection scheme is installed in the system from the start. Personal data is therefore protected without deliberate action by the individual. There is no need for the individual to change the settings. |
| Privacy Embedded into Design | The privacy protection scheme is integrated into the design and structure of the business and system. There is no need to add functions after start-up. The privacy protection scheme is a central and vital function for the business or system. |
| Positive-Sum, Not Zero-Sum | Rather than the zero-sum approach, in which the installation of a privacy protection scheme becomes a trade-off with convenience, the aim is the positive-sum approach that covers all fair benefits and goals. For the business enterprise, respect for privacy provides various incentives such as better customer satisfaction, better reputation and commercial profit. |
| Exhaustive Security | Data is protected throughout the lifecycle. Privacy-related information must be protected with solid security from creation until |

| | |
|---|---|
| | disposal. All data must be protected under data lifecycle control and disposed of without fail after the end of the process. |
| Visibility and Transparency | Visibility and transparency must be ensured in the privacy protection scheme and operations. Regardless of the business operation or technology, functionality of the privacy protection scheme is guaranteed for all interested parties. Here, system configuration and functions should be visible and verified for all users and providers. |
| Respect for User Privacy | The greatest respect should be paid to user privacy and the individual is at the center of attention. Standard and effective means to assure privacy protection, appropriate notice, and optional means that can easily enable the granting of authority are provided to the designer and manager of the business operation, to maintain the interests of the individual user to the maximum |

Source: Compiled by the Secretariat based on Privacy by Design: The Seven Foundational Principles

Privacy by Design adopts a positive-sum approach that aims to realize all fair profit and targets, such as various incentives that lead to increased corporate value through the respect for privacy, rather than a zero-sum approach that creates a trade-off in convenience with the implementation of a privacy protection scheme.

On the other hand, changes in business and social environments are likely to cause privacy problems that were not foreseen at the start. In such a case, having Privacy by Design in place at the start does not necessarily mean that protection is adequate. For this reason, it is necessary to study the construction of the mechanism based on Privacy by Design as well as the process of continual review and improvement.

# 8. Conclusion

In the future, data utilization is expected to be the fountainhead for the continued development of innovations and a core component in future corporate activities, including the realization of Society 5.0.

Of the data expected to be utilized, personal data is the fountainhead of business. However, privacy protection is essential in the pursuit of safety and security for users. In the promotion and realization of digital transformation (DX), assurance of trust is vital, and privacy protection as part of this effort is important. Although business enterprises in Japan have engaged in assuring privacy protection in earnest, many have been addressed with case-by-case actions. As the scope of data to be handled broadens, issues associated with privacy are expected to grow in diversity and complexity. The conventional approach to such issues is expected to be limited in effect, requiring a more strategic and organized approach. As interest in privacy grows, society, including consumers, has started to assess and distinguish rigorously business enterprises from the viewpoint of privacy. If a problem related to privacy occurs in activities conducted by a business enterprise, this will not only affect the activity in question but may have a serious impact on the entire business organization. Conversely, business enterprises that are handling privacy issues appropriately will gain trust from society, which will then lead to such business enterprises taking advantages in business. In other words, privacy handling has become vital for business enterprises and cannot necessarily be perceived as a cost. Rather, it is an activity that contributes to improvement in the quality of products and services and becomes a key discriminating factor *vis-à-vis* competitors.

For this reason, business enterprises are required to take organization-wide action in protecting privacy; that is, as part of governance. This Guidebook has been written for business leaders and the officers responsible for management strategies and support to identify the requirements and the organizational system that should be addressed by business leaders as part of their corporate privacy governance required in the future. In addition, privacy issues cannot be resolved independently by business enterprises. Rather, the importance of building their relationship and trust with society as a whole, including consumers, which can be maintained via resources such

as corporate notices, releases on privacy-related activities, and communications with consumers, has been acknowledged.

With business enterprises taking steps to accelerate DX, this Guidebook was created with the objective of contributing to privacy-related activities of business enterprises and, as a result, seeks to enhance the value of the products and services of a business enterprise and the economic and social value of the business enterprise.

It must be noted also that privacy issues not only depend on the target products and services but also in technological advances and social interest. In this respect, this Guidebook is expected to be revised and updated as the need dictates.

# Bibliography


- Survey on Privacy Governance (Overview) (JIPDEC, 2021), available only in Japanese
  - JIPDEC Press Release: https://www.jipdec.or.jp/topics/news/20211018.html
- Society 5.0 (Cabinet Office Website) https://www8.cao.go.jp/cstp/english/society5_0/index.html
- OECD Principles on AI (OECD, 2019) https://www.oecd.org/going-digital/ai/principles/
- Social Principles of Human-Centric AI (Council for Science, Technology and Innovation, 2019) https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf
- AI Utilization Guidelines (Ministry of Internal Affairs and Communications, 2019) https://www.soumu.go.jp/main_content/000658284.pdf
- Guidance on social responsibility (ISO26000: 2010) https://www.iso.org/standard/42546.html
- Guidance on social responsibility (JIS Z 26000: 2012)
- Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (A/HRC/17/31, 21 March 2011) https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.31_en.pdf
- The National Action Plan on Business and Human Rights (2020-2025)(the Inter-Ministerial Committee for Japan's National Action Plan (NAP) on Business and Human Rights, 2020), available only in Japanese https://www.mofa.go.jp/mofaj/press/release/press4_008862.html
- Report on Research on Business and Human Rights (Ministry of Justice, 2021), available only in Japanese https://www.moj.go.jp/JINKEN/jinken05_00045.html
- Guidelines on Respecting Human Rights in Responsible Supply Chains (Ministry of Economy, Trade and Industry, 2022) https://www.meti.go.jp/english/press/2022/pdf/0913_001a.pdf
- Principles for Responsible Institutional Investors [Japan's Stewardship Code] (Financial Services Agency, 2020 revision)

https://www.fsa.go.jp/en/refer/councils/stewardship/20200324/01.pdf

- Japan's Corporate Governance Code: Seeking Sustainable Corporate Growth and Increased Corporate Value over the Mid- to Long-Term (Tokyo Stock Exchange, Inc., 2021 revision) https://www.jpx.co.jp/english/news/1020/b5b4pj0000046kxj-att/b5b4pj0000046l07.pdf
- MSCI ESG Ratings Methodology: Privacy & Data Security Key Issue (MSCI ESG Research LLC, 2022) https://www.msci.com/documents/1296102/34424357/MSCI+ESG+Ratings+Methodology+-+Privacy+%26+Data+Security+Key+Issue.pdf/562b0a5b-b0ec-8bab-23dc-1c14967a08dc?t=1666182600406
- Expanding testing for the Privacy Sandbox for the Web (Google LLC, 2022) https://blog.google/products/chrome/update-testing-privacy-sandbox-web/
- The Use of Camera Systems with a Facial Recognition Function for Crime Prevention and Assurance of Safety (Personal Information Protection Commission, 2023), available only in Japanese https://www.ppc.go.jp/files/pdf/kaoshikibetsu_camera_system.pdf
- Case Studies on Review of the New Form of Data Distribution Trade ver.2.0 (Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications, IoT Acceleration Consortium, 2018), available only in Japanese
  - METI Press Release: https://warp.da.ndl.go.jp/info:ndljp/pid/11623215/www.meti.go.jp/press/2018/08/20180810002/20180810002.html
  - MIC Press Release: https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000045.html
- Case Studies on Review of the New Form of Data Distribution Trade First Volume (Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications, IoT Acceleration Consortium, 2020-2022), available only in Japanese https://www.meti.go.jp/policy/it_policy/privacy/privacy.html#data
- Guidebook for Utilization of Camera Images Ver.2.0 (IoT Acceleration Consortium, Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications, 2018), available only in Japanese

- METI Press Release: https://warp.da.ndl.go.jp/info:ndljp/pid/11067906/www.meti.go.jp/press/2017/03/20180330005/20180330005.html
- MIC Press Release: https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000040.html

· Guidebook for Utilization of Camera Images: Collection of Samples Pertaining to Advance Reporting and Notification (IoT Acceleration Consortium, Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications, 2019), available only in Japanese
- METI Press Release: https://warp.da.ndl.go.jp/info:ndljp/pid/12232105/www.meti.go.jp/press/2019/05/20190517001/20190517001.html
- MIC Press Release: https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000066.html

· Matters of Concern in Action by Private Business Operators for Public-Interest Purpose Utilizing Camera Images: Study in cases of infection countermeasure use (IoT Acceleration Consortium, Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications, 2021), available only in Japanese
- METI Press Release: https://warp.da.ndl.go.jp/info:ndljp/pid/12232105/www.meti.go.jp/press/2020/03/20210319007/20210319007.html
- MIC Press Release: https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000113.html

· Guidebook for Utilization of Camera Images Ver.3.0 (IoT Acceleration Consortium, Ministry of Economy, Trade and Industry and Ministry of Internal Affairs and Communications, 2022), available only in Japanese
- METI Press Release: https://warp.da.ndl.go.jp/collections/content/info:ndljp/pid/12323307/www.meti.go.jp/press/2021/03/20220330001/20220330001.html
- MIC Press Release: https://warp.da.ndl.go.jp/info:ndljp/pid/12213407/www.soumu.go.jp/menu_news/s-news/01kiban18_01000152.html

- GOVERNANCE INNOVATION: Redesigning Law and Architecture for Society 5.0 (Ministry of Economy, Trade and Industry, 2020) https://www.meti.go.jp/press/2020/07/20200713001/20200713001-2.pdf
- GOVERNANCE INNOVATION Ver. 2: A Guide to Designing and Implementing Agile Governance (Ministry of Economy, Trade and Industry, 2021) https://www.meti.go.jp/press/2021/07/20210730005/20210730005-2.pdf
- Agile Governance Update -How Governments, Businesses and Civil Society Can Create a Better World By Reimagining Governance- (Ministry of Economy, Trade and Industry, 2022) https://www.meti.go.jp/press/2022/08/20220808001/20220808001-b.pdf
- AI Governance in Japan Ver. 1.1: Report from the expert group on how AI principles should be implemented (Ministry of Economy, Trade and Industry, Japan, 2021) https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_8.pdf
- Governance Guidelines for Implementation of AI Principles ver. 1.0 (Ministry of Economy, Trade and Industry, Japan, 2021) https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20210709_9.pdf
- Ideal Protection and Utilization of Personal Data toward Society 5.0, (KEIDANREN, Japan Business Federation, 2019) https://www.keidanren.or.jp/en/policy/2019/083.html
- Outline: Ideal Protection and Utilization of Personal Data toward Society 5.0 (KEIDANREN, Japan Business Federation, 2019) https://www.keidanren.or.jp/en/policy/2019/083_outline.pdf
- Management Manifesto on Proper Utilization of Personal Data (KEIDANREN, Japan Business Federation, 2019) https://www.keidanren.or.jp/en/policy/2019/083_outline.pdf#page=14
- Information technology — Governance of IT for the organization (ISO/IEC 38500:2015)
- Information technology-Corporate governance of information technology (JIS Q 38500:2015)
- Act on the Protection of Personal Information "The Every-Three-Year Review" Outline of the System Reform (Personal Information Protection Commission, 2019)

https://www.ppc.go.jp/files/pdf/APPI_The_Every_Three_Year_Review_Outline_of_the_System_Reform.pdf
- Personal information protection management systems – Requirements (JIS Q 15001:2017)
- Information technology -- Security techniques -- Information security management systems – Requirements (ISO/IEC 27001:2013)
- Information technology -- Security techniques -- Information security management systems – Requirements (JIS Q 27001:2014)
- Information technology -- Security techniques -- Code of practice for information security controls (ISO/IEC 27002:2013)
- Information security, cybersecurity and privacy protection - Information security controls (JIS Q 27002:2014)
- Security techniques -- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -- Requirements and guidelines (ISO/IEC 27701: 2019)
- Guideline on Smart Home IoT Data Privacy (Smart Home Board, Japan Electronics and Information Technology Industries Association, 2023), available only in Japanese
https://home.jeita.or.jp/smarthome/iot/index.html
- Information technology — Security techniques — Privacy framework (ISO/IEC 29100: 2011)
- Information technology — Security techniques — Privacy framework (JIS X 9250:2017)
- Information technology — Security techniques — Guidelines for privacy impact assessment (ISO/IEC 29134: 2017)
- Information technology -- Security techniques -- Guidelines for privacy impact assessment (JIS X 9251: 2021)
- Promoting the implementation of PIA – Significance of PIA and Points to Keep in Mind in the Implementation Procedure – [Summary] (Personal Information Protection Commission, 2021), available only in Japanese
https://www.ppc.go.jp/files/pdf/pia_overview.pdf
- Promoting the implementation of PIA – Significance of PIA and Points to Keep in Mind in the Implementation Procedure – (Personal Information Protection Commission, 2021), available only in Japanese
https://www.ppc.go.jp/files/pdf/pia_promotion.pdf
- UNDERSTANDING PRIACY (DANIEL J. SOLOVE, 2008)

- A Taxonomy of Privacy (DANIEL J. SOLOVE, University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006, GWU Law School Public Law Research Paper No. 129), *available at* SSRN: https://ssrn.com/abstract=667622
- Final Recommendations on Profiling (Personal Data +α Study Group, 2022), available only in Japanese https://wp.shojihomu.co.jp/wp-content/uploads/2022/04/ef8280a7d908b3686f23842831dfa659.pdf
- Privacy by Design The 7 Foundational Principles (Ann Cavoukian, Information & Privacy Commissioner Ontario, Canada, 2011) https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf

## Review Organization

This document compiles the results of reviews conducted from FY2019 to FY2022 by the Corporate Privacy Governance Model Study Group chaired by Ichiro Satoh, Professor of the National Institute of Informatics, under the Data Distribution Promotion Working Group of the IoT Acceleration Consortium (chaired by Hiroyuki Morikawa, Professor of the University of Tokyo Graduate School).

**Figure 20. Members of the Corporate Privacy Governance Model Study Group**

| Status | Name (Honorifics omitted) | Organization |
|---|---|---|
| Chair | Ichiro Satoh | National Institute of Informatics |
| Member | Yoichiro Itakura | Hikari Sogoh Law Offices |
| | Masato Ochiai | Sompo Risk Management Inc. |
| | Tatsuya Kurosaka | Kuwadate,Inc |
| | Shintaro Kobayashi | Nomura Research Institute, Ltd. |
| | George Shishido | Graduate Schools for Law and Politics, The University of Tokyo |
| | Katsumi Takahashi | NTT Social Informatics Laboratories |
| | Tatsuya Hayashi | LocationMind Inc.<br>Parongo, Inc |
| | Tomomi Hioki | Miura & Partners |
| | Hisato Hiraiwa | PricewaterhouseCoopers Aarata LLC |
| | Yukiko Furuya | Nippon Association of Consumer Specialists / Consumer Conference For Sustainability |
| | Yosuke Murakami | KDDI Research, Inc. |
| | Ryoji Mori | Eichi Law Offices |
| | Mitsuo Wakameda | Keidanren (Japan Business Federation)<br>The Japan Research Institute, Limited |