IIAI Open Conference Publication Series
IIAI Letters on Business and Decision Science
Vol. 004, LBDS192
DOI: https://doi.org/10.52731/lbds.v004.192

Survey of the Act on the Protection of Personal Information in Japan and International Standard Framework for De-identification

Sanggyu Shin *

Abstract

This paper discusses the law definitions of de-identification, re-identification, anonymization, and pseudonymization based on Japan's amendment act of the Act on the Protection of Personal Information. It also introduces the current international standardization trends in de-identification, including the standardized framework ISO/IEC 27559 and ITU-TSG17 X.1148, and related international standards, ISO/IEC 20889, etc. Personal data de-identified by anonymization or pseudonymization must be de-identified adequately before being used as part of publicly available big data sets. Dealing with Big Data and sensitive personal data requires knowledge and technical competence to maintain the appropriateness of that data. Many companies are implementing Big Data projects and need a sound legal understanding to develop in line with international standards to remain compliant with the ever-increasing regulatory risk requirements.

Keywords: Act on the Protection of Personal Information, de-identification, ISO/IEC 20889, ISO/IEC 27559, ITU-TSG17 X.1148

1 Publication Principle

The recent boom of ChatGPT and Generative AI is based on collecting and analyzing vast amounts of data. Thus, with the recent arrival of the 5G era, the demand for economic revitalization of the "data" industry, which is the core resource of the 4th industrial revolution and an essential element for revitalizing new industries such as AI, cloud computing, and the IoT, is increasing. However, in data collection and utilization by companies and institutions, the possibility of invasion of personal privacy is also increasing. While the collected Big Data has become a seed of technological development through its explosive use in intellectual data science, science, technology, and humanities, it has also raised various technical and legal issues in its development, such as personal information issues and copyright issues of the collected data [1][2][3].

Big data is legally defined as publicly accessible data that can only be used if adequately disseminated and anonymized. In order to promote its use within legal limits, it is necessary to understand and propose new standard technologies for de-identification (anonymization and pseudonymization) and re-identification to facilitate and manage the introduction of standardization of development frames related to the field of Big Data.

Sweeney's study proved that 87% of the U.S. population can be uniquely identified based on gender, zip code, and date of birth [4]. In another research, the EFF (Electronic Frontier

* Tokai University, Tokyo, Japan

Foundation) research team collected and analyzed anonymous AOL search queries in 2006 and identified individuals from de-identified Netflix usage data. This indicates that data processing by anonymization is practical and valuable in many fields but requires further research and considerable caution.

The process of de-identification, represented by anonymization, is modifying identifiable data so that specific individuals cannot be identified. Research on technical methodologies for increasing the de-identification level without compromising the data's usefulness is actively conducted in the de-identification field. In addition, there is a need to develop requirements for data de-identification assurance to determine the appropriate level of de-identification depending on the environment of de-identification processing and the purpose of processing.

This paper discusses the law definition of de-identified information according to the amended *Act on the Protection of Personal Information* (Act No. 37 of 2021) (referred to as "APPI"), enforced from April 1, 2022 [5]. This paper also introduces the international standards and standardization promotion trends developed to present the framework and data de-identification evaluation requirements currently standardized in the de-identification field.

First, Chapter 2 explains the APPI, Chapter 3 describes the concept of the de-identification process and the definition and differences of each piece of personal information based on the Act, Chapter 4 summarizes international standardization movements related to non-identification processes and concludes in the last chapter.

2 Act on the Protection of Personal Information

Recently, the problems related to the collection of personal information by ChatGPT and the privacy protection of Internet advertisements have become a common topic of discussion [6]. The EU and the U.S. were the fastest countries to address the issue of privacy protection on the internet, and now Japan has enacted the APPI (Act No. 57 of 2003) promulgated in 2003, and it was enforced from April 1, 2005. In 2017, 2022, and 2023, this APPI (Last Version: Act No. 37 of 2021) was revised and enforced [5].

Worldwide, the direction of revising the act about personal information protection is to expand individuals' rights and interests and strengthen regulations. However, there are also some attempts to expand the scope of personal information and new regulations that directly affect companies that handle information, such as creating pseudonym processing information to promote the utilization of personal data and the mandatory reporting of information leaks.

The information used by processing personal data is statistical and anonymously processed information. In 2022, the revised APPI in Japan added a new type of processed information. Among the various new regulations, personal information is among the most crucial laws regarding companies' digital marketing practices. First, this paper introduces the legal definition of the difference between personal information, personal related information, anonymously processed information, and pseudonymously processed information.

A summary of the amendment act of the APPI enforced on April 1, 2022 and 2023, is as follows [7][8][9].

1. Protection of individual rights and interests.
2. Enhanced protection and utilization through the results of technological innovation.
3. Harmonization and coordination with international systems.
4. Responding to new risks associated with increased cross-border data distribution.

5. Responding to the era of AI and big data.

At this amendment act on the APPI, the following personal information protection system items were reviewed [10].

1. In addition to integrating the three laws of the APPI, the APPI Held by Administrative Organs, and the APPI Held by Incorporated Administrative Agencies, etc., into one amendment act of the APPI law, it stipulates standard nationwide rules for local governments' personal information protection systems. It also unifies the entire jurisdiction under the PPC (Personal Information Protection Commission, Japan) [11].
2. In principle, the same rules apply to public and private hospitals and universities, etc., to unify regulations in medical and academic fields.
3. To make provisions, including the ones in the area of academic studies in line with requirements for the adequacy decision under the GDPR (General Data Protection Regulations) [12], across-the-board exemption provisions to all obligations in the area of academic studies will be reviewed, and exemption provisions to several commitments will be put in place.
4. Standardize the definition of personal information in the national government, private sector, and local governments, and clarify the rules regarding handling anonymously processed information by government agencies, etc.

2.1 Each Legal Terms and Definitions

The amendment act of the APPI defines in detail what *Personal Information* is, so as to remove any gray areas. Personal information refers to information relating to a living individual that can identify a specific individual by name, date of birth, etc., or contains an individual identification code[†]. Personal information includes information that can be readily collated with other data and thereby identify a specific individual [5][8][9].

According to the APPI definition, the *Information related to Personal Information* is defined passively as "the information relating to a living individual which doesn't fall under personal information, pseudonymized personal information, and anonymized personal information." Generally speaking, this includes internet browsing history, location information, cookie information, etc., not linked to personal information such as names. The information obtained by cookies is not personal but is treated as personally identifiable under the revised law [5][8][9].

Statistical Information is obtained by extracting common elements from the information of multiple persons and aggregating them in the same category. It generally does not fall under the category of personal information because it excludes any correspondence with specific individuals [14][15]. Since the Personal Information Protection Law does not explicitly regulate statistical information, it can be freely used for any purpose and provided to any third party. Therefore, if customers and users consent to provide their data to third parties, a provider can offer them both the as-is personal data and the data with a certain level of processing. However, it takes work to obtain consent to provide personal data to third parties again [16].

[†] Personal information refers to the information that is converted into the characteristics of a part of the body for computer use (e.g., DNA, face, etc.) and the number assigned to a service user for the benefit of public services (e.g., driver's license number, my number [13], etc.).

2.2 The Need to Amend the Law

In the EU, the GDPR (General Data Protection Regulation), the law governing personal data protection, came into effect in 2018 (enacted in April 2016) due to concerns about privacy on the internet. The GDPR replaces the EU Data Protection Directive 95 [17], the law governing the protection of personal data within the EU, which has been applied from 1995 to the present. The GDPR is stricter than the EU Data Protection Directive, which stipulates that online identifiers such as IP addresses and cookies are included in personal data. In addition, companies must now obtain explicit consent from users to use their personal information [12][18].

The GDPR was one of the triggers that further stimulated the discussion on privacy worldwide. In 2020, California in the U.S. enacted its law, the CCPA (California Consumer Privacy Act) [19][20]. In addition, South Korea[‡], Brazil and other countries are also planning or considering enforcing similar laws to enact their privacy laws.

In the industrial world, technical restrictions by platforms such as Apple and Google's restriction on using 3rd party cookies are also in progress [22].

In Japan, the law on protecting personal information (officially called the "Act on the Protection of Personal Information") was enforced in 2005. The recent development of the internet and its accompanying increasingly widespread use of data by companies have brought about significant changes in the environment in which personal information is handled. In order to respond to these changes in the environment, the law has had to undergo significant changes in content to keep up with the times.

Based on "The Every-Three-Year Review" provisions, Article 12 of the Supplementary Provisions of the 2015 Amendment Act, the APPI has been reviewing every three years in the Supplementary Provision of the revised law [5]. Additionally, the review is conducted when necessary in light of international trends in protecting personal information, the progress of information and communication technology, and the creation of new industries in line with such developments. Accordingly, the first revision of the Act on the Protection of Personal Information was promulgated in 2017, and the second revision of the Act on the Protection of Personal Information was enacted in June 2020 and came into effect in April 2022[5][9].

3 De-identification Process

The enforced APPI from Apr. 2022 newly defined *Pseudonymized Personal Information* to promote the utilization of personal data. Thus, it is necessary to understand the difference between *Anonymized Personal Information* and *Pseudonymized Personal Information*.

3.1 Concept of de-identification

Both anonymously processed information and pseudonymously processed information are related to de-identification. The de-identification information is defined as "information about an individual obtained by processing personal information so that the individual cannot be identified

[‡] Korea's amended decree of the *Personal Information Protection Act*, which went into effect on September 15, 2023, includes various contents discussed in multiple fields, such as unifying the online-offline personal information processing standards into a digital environment while practically guaranteeing the rights of citizens as information subjects [21].

and the personal information cannot be restored" by deleting a part of descriptions, etc., included in the personal information or deleting all personal identification codes, etc.

3.2 Anonymization

Anonymized personal information was newly introduced by the amendment act of the APPI in 2015 to promote the use of personal data, including data transactions and data linkage between businesses, under specific rules and without the individual's consent.

The anonymized processed information is "information on individuals obtained by processing[§] personal information so that specific individuals cannot be identified, and such personal information cannot be restored." Additionally, it means the information that the particular individual cannot be re-identified by restoring that processed information [5].

Therefore, anonymous processing means the information is processed so that individuals cannot be identified by any reasonably foreseeable means (cost, time, and technological development). Since anonymous information is not personal information, it is not subject to the Personal Information Protection Law and can be used freely.

However, even if an administrator anonymizes anyone's personal data, people still do not know what other data is out or flow on the internet, etc., about them, as outlined by the UK ICO (Information Commissioner's Office) in its own Anonymization Standards Guide [23]. The problem remains that people never know how someone else might map it to an anonymous dataset.

3.3 Pseudonymization

In the 2020 amendment act, from the perspective of promoting innovation, "Pseudonymized Personal Information," which is the personal information that has been processed so as not to be able to identify a specific individual unless collated with other information, is established, which eases the obligation to respond to requests (by taking any of the measures prescribed in each processing[§] by the divisions of personal information outlined in those items) for disclosure and suspension of use, provided that the personal information handling business operator must limit its use to internal analysis [5].

The following reasons are given in the "Guidelines on the APPI (Pseudonymized and anonymized processed information version)" as the reasons why the new pseudonymized information was newly established by the draft amendment to the Personal Information Protection Law approved by the Cabinet in March 2020, even though anonymized processed information existed in the past [24].

- Because there are some cases in which some business operators use personal information after processing it into "pseudonymization."
- The EU has stipulated "pseudonymization," which allows slightly loose handling of personal information while assuming that it is handled as personal information, and its use has been increasing internationally.

---

§ 1) Deleting a part of the identifiers or their equivalent contained in the personal information (including replacing the part of the identifiers or their equivalent with other identifiers or their equivalent without following patterns that enable its restoration) or
2) Deleting all individual identification codes contained in the personal information (including replacing the individual identification codes with other identifiers or their equivalent without following patterns that enable restoration of the individual identification codes) [5].

In other words, introducing pseudonymized information, which is information processed so that a specific individual cannot be identified without cross-checking with additional details, promotes further utilization of such information while ensuring a certain level of security. Therefore, pseudonymization is processing personal information so that a specific individual cannot be identified without additional information. In other words, it replaces the data set's identifiers with other attributes by using encryption, hashing, or other methods. Pseudonymized information is subject to the APPI because it is personal information that can be used with technical and administrative security measures for limited purposes.

3.4 Differences between each type of information

Both pseudonymized and anonymized information have in common that they are created by processing personal information or identification codes. The main difference is whether or not the information can be provided to a third party. Suppose someone wants to provide anonymized processed or statistical information to a third party without the owner's consent. In that case, the user should use anonymized processed or statistical information, while providing pseudonymized processed data to a third party is prohibited under any circumstances.

Suppose someone wants to change the purpose of use without the owner's consent. In that case, the user can use pseudo-processed, anonymized, processed, and statistical information. However, pseudo-processed information can be used only for the same company, subcontractors, and joint use, while the use with access to the original individual is prohibited. The differences in the information are shown in Table 1.

Table 1: Differences between each type of information

	Personal Information	Statistical Information	Anonymized Processed Information	Pseudonymized Processed Information
Provision to 3rd Parties	○ Consent required	◎ Consent not required	◎ Consent not required	×
Change of purpose of use	-	◎ Consent not required	◎ Consent not required	◎ Consent not required
Re-identification	-	Not possible	Prohibited	Prohibited
Response to requests for disclosure, stop using, etc.	Necessary	Not necessary	Not necessary	Not necessary
Reporting of leaks, etc.	Necessary	Not necessary	Not necessary	Not necessary

3.5 Re-identification Issues

Concerns about re-identification surfaced in 2021 when the UK's NHS Digital (Centre for Health and Social Care Information) pushed for large-scale health data collection on the British public under the "General Practice Data for Planning and Research" initiative. The plan was to transmit and consolidate the GP medical records of the entire population of England to a central research institute, and the public was given only a short window of time to opt-out[**].

In Japan, there is a privacy-related case of East Japan Railway Company, which provided users' usage history to a third party, Hitachi, Ltd., in 2013.

One of the theoretical ways to overcome the re-identification problem is to keep removing data that reveals the identity of individuals. However, the value of the dataset decreases each time the data is removed. One way to achieve both anonymity and usefulness is differential privacy. This method adds statistical noise to the data by subtly changing parameters. For example, by shifting a person's age or zip code slightly, it isn't easy to correlate them. However, researchers and hackers can eliminate the noise by repeatedly accessing the database. As a countermeasure, another element of differential privacy is to limit the number of times the data can be accessed.

Legally, there is a direction to seek further development of laws on de-identification, but it is an administrative measure, not a technical one.

4 International Standardization Movement

ISO/IEC JTC 1/SC 27/WG 5 is a standardization group developing international standards related to personal information protection. The group is developing international standards such as the Privacy Framework (ISO/IEC 29100:2011 [25][26]), Guidelines for privacy impact assessment (ISO/IEC 29134:2023 [27]), Code of practice for personally identifiable information protection (ISO/IEC 29151:2017 [28]), Privacy enhancing data de-identification terminology and classification of techniques (ISO/IEC 20889:2018 [29]), Privacy enhancing data de-identification framework (ISO/IEC 27559:2022 [30]), etc. In particular, the data de-identification framework is a standard closely related to pseudonymization.

4.1 ISO/IEC 20889:2018

The ISO/IEC 20889:2018 [29] is the first international standard of the de-identification field. ISO/IEC JTC1 developed this standard, and it describes privacy-enhancing data de-identification techniques, to be used to describe and design de-identification measures in accordance with the privacy principles in ISO/IEC 29100:2011 [25][26]. This standard describes the characteristics of the essential technologies and the applicability of each technology to reduce the risk of re-identification using standardized terminology by the personal information protection principles of ISO/IEC 29100.

The main contents of this standard include types of re-identification attacks, types of de-identification techniques, general privacy measurement models, general principles for applying de-identification techniques, and the introduction of characteristics of de-identification tools,

[**] They are sending promotional advertisements by email or other means without the user's permission. Also, the user must indicate his/her intention to refuse to receive the advertisements.

techniques, and models. On the other hand, the techniques presented in ISO/IEC 20889 apply to data sets that can be converted into table format but not to complex data sets, including free-form text, images, audio, and video. The most important feature of the standard is that if there is a de-identification technique that can help to counteract the same attack risk, the best technique should be selected from the viewpoint of usefulness, taking into account multiple techniques and risks from a quantitative viewpoint, etc. [29].

ISO/IEC 20889, as mentioned above, describes privacy-enhanced data de-identification techniques used in the description and design of privacy protection measures based on the privacy protection principles of ISO/IEC 29100.

ISO/IEC 29100:2011 specifies the following personal information security framework [25][26],

- Specifies common privacy terms,
- Defines who processes personally identifiable information (PII) and their roles,
- Describes privacy considerations,
- Provides references to known privacy principles for information technology.

ISO/IEC 29100:2011 applies to natural persons and organizations involved in the specification, procurement, design, development, testing, maintenance, management, and operation of information and communication technology systems and services requiring privacy controls for PII processing [25].

4.2 ISO/IEC 27559:2022

International Standard ISO/IEC 27559:2022is a standard that has progressed from the ISO and IEC Joint Technical Committee (JTC1) SC27 WG5. It is being established as a follow-on standard to the ISO/IEC 20889 Privacy Enhanced Data De-identification Terminology and Technical Classification, an international standard established in November 2018 [30].

The ISO/IEC 27559 standard provides a framework for understanding and mitigating risks associated with the lifecycle of de-identified data. This document describes the considerations that must be made for de-identification to contribute to improved privacy. Whereas ISO/IEC 27551:2021 lays out the concept of what is meant by deconsolidation (e.g., anonymization), this standard lays out the specific things that should be done [31].

Table 2 shows the structure of the de-identification framework in 27559. This document provides organizations with an implementation framework to govern the appropriate use of data de-identification techniques described in ISO/IEC 20889. This de-identification framework can be applied at any point in the data lifecycle, from designing the means of data collection to internal reuse, making data available to external partners, or archival.

4.3 ITU-TSG17 X.1148

The ITU-TSG17 X.1148 Framework of de-identification process for telecommunication service providers [32] was developed by the FSI (Financial Security Institute) in Korea and the KISA (Korea Internet Security Agency) in the ITU-T SG17 (Information Protection). At the 2016 SG

Table 2: Composition of the de-identification framework [30]

Elements	Main contents
Context	The environment and context in which the recipient can use the data are assessed to determine the external information that an attacker can exploit. This means that context-aware controls can manage risks (recipient's IT security controls, obligations described in written contracts, policies, and governance measures).
Data	Evaluate the data itself to determine how additional information available to an attacker can be used to represent or reveal PII. Risk can be managed by limiting what data can be leveraged through data transformation and what data formats can be leveraged in the future.
Identifiability	The method to evaluate identifiability is determined by context risk (probability of an attack) and data risk (probability of disclosure in case of attack). For the identifiability to be less than a predefined tolerance level, it is necessary to define an appropriate tolerance.
Governance	This means the procedures and practices documented by management to ensure that the above are completed consistently and efficiently now and in the future, before the availability of de-identified data is ensured, of the process of ensuring it, and of the preparations required after it is ensured.

17 Regular Meeting, Korea's FSI, ETRI (Electronics Telecommunications Research Institute), Soon Chun Hyang Univ. of Korea, and China Mobile of China participated as co-editors, and this is a proposal adopted as a new possible task.

In August 2016, the Korea Internet Promotion Agency was officially designated as the Support Center for De-Identification Measures and joined as a co-editor of this standard in December, and both organizations are currently taking the lead in establishing the standard.

This standard is an international standard for de-identification procedures and applies to all industrial fields. However, detailed techniques for de-identification processing are not dealt with separately because they overlap in scope with ISO 20889.

The three main contents of this de-identification procedure standard are as follows [32].

1. Definition of the points where de-identification processing is required based on the data flow (life cycle).
2. The four-step de-identification procedure is presented in the Korean guideline.
3. Data format according to the characteristics of each de-identification information provision model and the level of de-identification processing.

Figure 1 is a diagram of the data form and de-identification level in the de-identification process. Figure 1 provides data stages from identified data to de-identified data in the de-identification process. Each stage has a different possibility of re-identification risk as a spectrum.

As shown in Figure 1, all data exist in the de-identification stage. At the right (the highest-level de-identification) are de-identified data unrelated to individuals (for example, historical weather

records) and therefore seek no privacy risk. At the left end (the lowest-level de-identification) are identified data linked directly to specific individuals. Between these two data stages are data that can be connected with effort, can only be linked to groups of people, and are based on individuals but cannot be linked back to them.

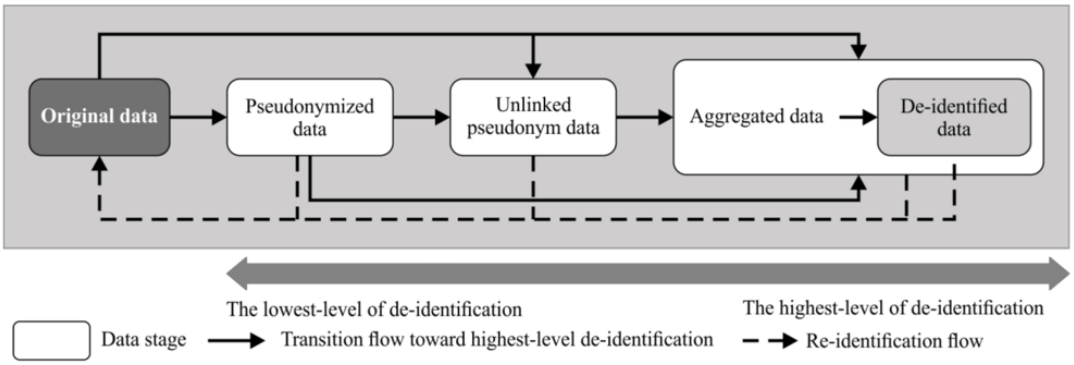

Figure 1: De-identified data stages [24]

5 Conclusion

In Japan, after several incidents of personal information leaks, it has become mandatory to apply anonymization, pseudonymization, and personal information filtering technologies when handling personal information.

The recent revision of the Personal Information Protection Law has added a legal basis for pseudonymized information, and we expect that the creation of de-identified information will also expand its use. To rapidly grow the economy by utilizing data, such as AI technologies for speech recognition, text generation, photo generation, and personalized data generation, the utilization of personal information will become more and more critical. The interest and development of de-identification and personal information protection technologies for stable utilization will be necessary along with the necessity of such utilization.

In particular, by studying the contents of international standards such as X.1148 and ISO/IEC 27559, which were finally adopted as international standards of de-identification framework, and the global movement toward standardization, we expect that we can correctly understand and utilize the de-identified information according to the requirements and that this will be useful for the economic utilization of data industry.

References

[1] Cabinet Office Site (Japan), “Society 5.0,” Dec. 2023; www8.cao.go.jp/cstp/english/society5_0/index.html.

[2] M. Alawida, S. Mejri, A. Mehmood, B. Chikhaoui, and O. I. Abiodun, “A Comprehensive Study of ChatGPT: Advancements, Limitations, and Ethical Considerations in Natural Language Processing and Cybersecurity,” Information 2023, vol. 14, issue. 8 (462); doi:10.3390/info14080462.

[3] A. Khanan, S. Abdullah, A. H. H. M. Mohamed, A. Mehmood, and K. A. Z. Ariffin, “Big

Data Security and Privacy Concerns: A Review," Smart Technologies and Innovation for a Sustainable Future, Springer, 2019 pp. 55–61.

[4] L. Sweeney, "Simple Demographics Often Identify People Uniquely," Data Privacy Working Paper 3, Carnegie Mellon University, Pittsburgh, Pennsylvania, 2000.

[5] Japanese Law Translation, "Act on the Protection of Personal Information (Act No. 57 of 2003)," Mar. 2023; www.japaneselawtranslation.go.jp/en/laws/view/4241/en.

[6] M. Gupta, C. Akiri, K. Aryal, E. Parker, and L. Praharaj, "From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy," IEEE Access, vol. 11, 2023, pp. 80218-80245; doi:10.1109/ACCESS.2023.3300381.

[7] Financial Services Agency (Japan), "Guidelines for the Act on the Protection of Personal Information," April 2007; www.fsa.go.jp/frtc/kenkyu/event/20070424_02.pdf.

[8] PPC (Personal Information Protection Commission, Japan), "Laws and Policies," Dec. 2023; www.ppc.go.jp/en/legal/.

[9] Ministry of Justice (Japan), "The Amendment Act of the Act on the Protection of Personal Information, etc. (Overview)," Sep. 2022; www.moj.go.jp/content/001345599.pdf.

[10] Japanese Law Translation, Outline of the Acton the Arrangement of Related Laws for the Formation of a Digital Society;
www.japaneselawtranslation.go.jp/outline/36/211105155408_905R305.pdf.

[11] PPC (Personal Information Protection Commission, Japan) Site; www.ppc.go.jp/en/.

[12] GDPR (General Data Protection Regulation) Site; https://gdpr-info.eu/.

[13] The Japan Agency for Local Authority Information System, Individual Number Card (My Number Card); www.kojinbango-card.go.jp/en/.

[14] PPC (Personal Information Protection Commission, Japan), "Report by the Personal Information Protection Commission Secretariat: Anonymously Processed Information," Feb. 2017;
www.ppc.go.jp/files/pdf/The_PPC_Secretariat_Report_on_Anonymously_Processed_Information.pdf.

[15] Ministry of Internal Affairs and Communications (Japan), "Guidelines for the Act on the Protection of Personal Information," PPC (Personal Information Protection Commission, Japan), 2016.

[16] Ministry of Internal Affairs and Communications Ministry of Economy, Trade and Industry (Japan), "The Guidebook for Corporate Privacy Governance in the Digital Transformation (DX) Era," April 2023;
www.meti.go.jp/policy/it_policy/privacy/guidebook_ver1.3_english.pdf.

[17] EUR-Lex, "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and

on the free movement of such data," May 2018; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

[18] PPC (Personal Information Protection Commission, Japan), GDPR (General Data Protection Regulation); www.ppc.go.jp/enforcement/infoprovision/EU/.

[19] R. Bonta, "State of California Department of Justice, California Consumer Privacy Act (CCPA)," May 2023; https://oag.ca.gov/privacy/ccpa.

[20] California Legislative Information, "California Consumer Privacy Act of 2018," Dec. 2020; https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[21] Korea Legislation Research Institute, "PERSONAL INFORMATION PROTECTION ACT," Oct. 2023; elaw.klri.re.kr/eng_service/lawView.do?hseq=62389&lang=ENG.

[22] A. Seipp, The End of Third-Party Tracking, The Rise of iOS14 ITP; mcgaw.io/blog/end-of-third-party-cookies-ios14-itp/#gs.0xj024.

[23] Information Commissioner's Office Site; https://ico.org.uk/.

[24] PPC (Personal Information Protection Commission, Japan), "Guidelines on the Act on the Protection of Personal Information (Pseudonymized and anonymized processed information version)," Sep. 2022 (Japanese); www.ppc.go.jp/personalinfo/legal/guidelines_anonymous/.

[25] ISO/IEC 29100:2011 Information technology - Security techniques - Privacy framework, Dec. 2011; www.iso.org/standard/45123.html.

[26] ISO/IEC 29100:2011/Amd.1:2018 Information technology - Security techniques - Privacy framework, June 2018; www.iso.org/standard/73722.html.

[27] ISO/IEC 29134:2023 Information technology - Security techniques - Guidelines for privacy impact assessment, May 2023; www.iso.org/standard/86012.html.

[28] ISO/IEC 29151:2017 Information technology - Security techniques - Code of practice for personally identifiable information protection, Aug. 2017; www.iso.org/standard/62726.html.

[29] ISO/IEC 20889:2018 Privacy enhancing data de-identification terminology and classification of techniques, Nov. 2018; www.iso.org/standard/69373.html.

[30] ISO/IEC 27559:2022 Information security, cybersecurity and privacy protection - Privacy enhancing data de-identification framework, Nov. 2022; www.iso.org/standard/71677.html.

[31] ISO/IEC 27551:2021, Information security, cybersecurity and privacy protection Requirements for attribute-based unlinkable entity authentication, 2021; www.iso.org/standard/72018.html.

[32] International Telecommunication Union, X.1148: Framework of de-identification process for telecommunication service providers, 2020; https://www.itu.int/rec/T-REC-X.1148-202009-I.