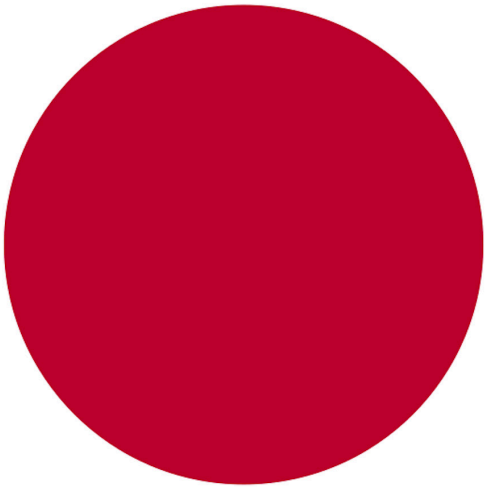
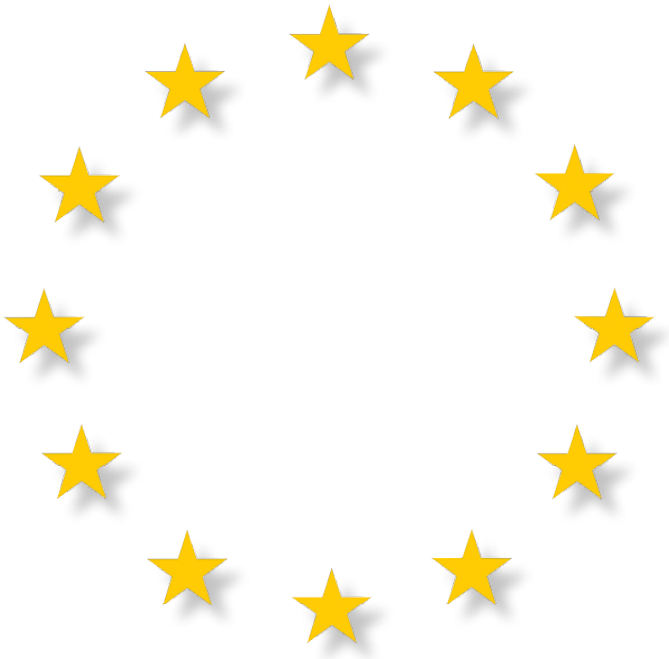
LATEST EDITION



Comparing privacy laws:
GDPR v. APPI



JUNE 2021

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

TMI Associates was established on October 1, 1990, with the aim of responding to the demand for comprehensive professional services required in the new era. TMI is comprised of attorneys, patent attorneys, paralegals and staff with extensive experience in both domestic and international practice. We have been actively engaging in business by opening oversea branch offices throughout the Asian region, such as in China, Vietnam, Singapore, Myanmar, Thailand and Cambodia, as well as our offices in Silicon Valley and London. Moreover, we have also placed TMI representatives in France, Brazil, Kenya, India, the Philippines and Indonesia. This provides a system which enables our team to suitably respond to our clients' needs for a wide range of legal services in a timely manner by taking advantage of our extensive array of practice areas, expertise and experience as a major law firm with the aim of achieving high levels of client satisfaction tailored to each locality.

OneTrust DataGuidance™ provides a suite of privacy solutions designed to help organisations monitor regulatory developments, mitigate risk and achieve global compliance.

The OneTrust DataGuidance™ platform includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Cross-Border Charts which allow you to compare regulations across multiple jurisdictions at a glance, a daily customised news service and expert analysis.

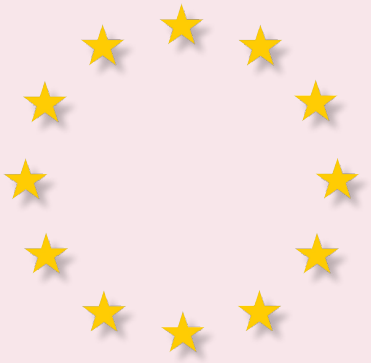
These tools, along with our in-house analyst service to help with your specific research questions, provide a cost-effective and efficient solution to design and support your privacy programme.

Contributors

OneTrust DataGuidance™
Keshawna Campbell, Angela Potter, Emily Dampster, Victoria Ashcroft

Image production credits:
Cover/p.5/p.51: cnythzl / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com

Table of contents



Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') and the Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2015) ('APPI') both aim to provide protections for individuals and their personal data, as well as requirements for businesses regarding the collection, processing, transfer, use, storage, and maintenance of customer and employee data.

The initial version of the APPI, developed in 2003, was one of the first data protection laws to be introduced in Asia. The APPI was significantly amended in 2016, and most recently in 2020. The bill to amend the APPI ('2020 Amendments') was passed by the National Diet of Japan ('Parliament of Japan') on 5 June 2020 and is set to enter into full effect on 1 April 2022, with the transitional measures for transferring personal data to a third party pursuant to Article 23(2) of the APPI, entering into effect on 1 October 2021. The 2020 Amendments introduce significant changes to the APPI including the introduction of the concept of pseudonymised personal information, mandatory breach reporting, expanded principal rights, and higher penalties for violations of the orders issued by the Personal Information Protection Commission ('PPC'). Further to this, a Bill on the Development of Related Laws for the Formation of a Digital Society was passed by the Parliament of Japan on 12 May 2021 and will make further amendments to the APPI.

Notably, on 23 January 2019, Japan became the first country in Asia to be granted adequacy status by the European Commission, following discussions with the PPC. This decision indicated that the APPI, in conjunction with other relevant provisions in Japanese law, provides an 'essentially equivalent' level of protection to personal data to that of the GDPR. As the adequacy decision and this Guide highlight, the APPI and GDPR have several similarities. In particular, both laws contain provisions for special or sensitive information, define personal data as information that can be used to identify an individual, include an extraterritorial scope, and establish obligations for operators or controllers/processors who handle personal data. In addition, the APPI and GDPR detail data subject rights including the right of erasure, to be informed, to object, to access personal data, and identify consent as a central principle. Both laws also provide for supervisory authorities and the issuing of financial sanctions.

At the same time, however, the APPI and GDPR differ in significant ways. Where the GDPR specifies a distinction between data controllers and processors, the APPI only refers to personal information controllers. The GDPR presents a detailed definition of processing, but the APPI only clarifies that it applies to personal information, personal information databases, and retained personal data. Certain provisions in the APPI apply to such retained personal data, while the GDPR does not make this differentiation. In contrast, the GDPR contains provisions regarding children, processing for research purposes, and specifications on how to obtain consent, which are not addressed in the APPI.

Furthermore, the GDPR provides for significantly larger financial penalties, up to €20 million or 4% of global annual turnover, compared to the APPI in which the maximum single fine is JPY 1 million (approx. €7,500). The APPI does, however, stipulate imprisonment as a potential penalty. Additionally, the APPI applies to anonymised data, while the GDPR explicitly excludes such data from its scope.

This Guide is therefore aimed at highlighting the similarities and differences between the two pieces of legislation in order to help organisations develop their compliance activities.

Structure and overview of the Guide

This Guide provides a comparison of the two pieces of legislation on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Individuals' Rights
5. Enforcement

Each topic includes relevant articles and sections from the two laws, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the APPI.

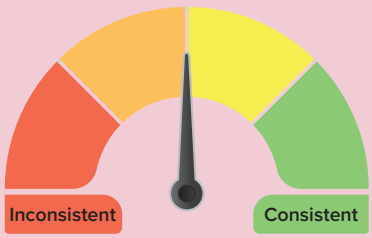
Key for giving the consistency rate

Consistent: The GDPR and APPI bear a high degree of similarity in the rationale, core, scope, and the application of the provision considered.

Fairly consistent: The GDPR and APPI bear a high degree of similarity in the rationale, core, and the scope of the provision considered; however, the details governing its application differ.

Fairly inconsistent: The GDPR and APPI bear several differences with regard to scope and application of the provision considered, however its rationale and core presents some similarities.

Inconsistent: The GDPR and APPI bear a high degree of difference with regard to the rationale, core, scope and application of the provision considered.



Usage of the Guide

This Guide is general and educational in nature and is not intended to provide, and should not be relied on, as a source of legal advice. The information and materials provided in the Guide may not be applicable in all (or any) situations and should not be acted upon without specific legal advice based on particular circumstances.

1. Scope

1.1. Personal scope

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') applies to data controllers and data processors, which may be businesses, public bodies, institutions as well as not for profit organisations. The Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2015) ('APPI') applies to a 'personal information controller' ('PIC') who is defined as a 'person providing a personal information database etc. for use in business.' Persons within public bodies, such as central government organisations, local governments, incorporated administrative agencies, and local incorporated administrative agencies are regulated by other laws and regulations.

Both the GDPR and APPI protect living individuals with regard to the use of their personal data. The GDPR provides that individuals are protected regardless of their nationality and/or residency, while the APPI does not explicitly address this point. However, the Guideline of the APPI (General Rules Edition) ('General Rules Guideline') published by the Personal Information Protection Commission ('PPC') states that individuals are protected regardless of their nationality and/or residency.

Please note that a bill to amend the APPI (only available in Japanese here; English summary available here) was passed by the National Diet of Japan on 5 June 2020 and was promulgated on 12 June 2020 ('2020 Amendment'). The amendments will enter into force on 1 April 2022, but the transitional measures for transferring personal data to a third party pursuant to Article 23(2) of the APPI will enter into effect on 1 October 2021. In addition, a Bill on the Development of Related Laws for the Formation of a Digital Society was approved by the Cabinet of Japan which will make further amendments to the APPI. Such amendment to the APPI is under consideration but is expected to pass by June 2021.

GDPR	APPI
Articles 3, 4(1) Recitals 2, 14, 22-25	Articles 1, 2(5), 2(8), 76

Similarities

GDPR	APPI
The GDPR **only** protects living individuals. Legal persons' personal data is not covered by the GDPR. The GDPR does not protect the personal data of deceased individuals, and instead leaves this to Member States to regulate.	The APPI only applies to the personal information of '**living individuals**.'
Article 4(1) of the GDPR clarifies that a **data subject** is 'an identified or identifiable natural person.'	Article 2(8) of the APPI clarifies that a '**principal**' is 'a specific individual identifiable by personal information.'
The GDPR provides that it 'should apply to natural persons, **whatever their nationality or place of residence**, in relation to the processing of their personal data.'	The APPI does **not** explicitly make any reference to a principal's nationality or place of residence. However, the General Rules Guideline states that individuals are protected **regardless of their nationality and/or residency**.

Differences

GDPR	APPI
The GDPR applies to a **data controller** which is defined by the fact that it establishes the **means** and **purposes of the processing**.	The APPI applies to a **PIC**, which is defined as a 'person providing a personal information database etc. for use **in business**.'

GDPR	APPI

Differences (cont'd)

The GDPR sets several obligations that apply to '**processors**,' which are entities that process personal data **on behalf of data controllers**.	The APPI **only** explicitly refers to **PICs** as being subject to its obligations.
The GDPR applies to businesses, **public bodies, institutions**, as well as **not for profit businesses**.	The APPI states that central government organisations, local governments, incorporated administrative agencies, and local incorporated administrative agencies are **excluded** from the definition of PIC (as specified in Article 2(5)). In addition, the following are **out of the scope of the obligations for PICs under the APPI**: broadcasting institutions, newspaper publishers, communication agencies, other press organisations, a person who practices writing as a profession, universities and other organisations or groups aimed at academic studies, as well as political and religious bodies (as specified in Article 76).

1.2. Territorial scope

Fairly consistent

Both the GDPR and the APPI have an extraterritorial scope. In particular, the GDPR applies to organisations outside the EU if they offer goods or services to, or monitor the behaviour of, individuals within the EU.

Some provisions of the APPI apply to business operators, who in relation to supplying a good or service to a person in Japan, have acquired personal information in Japan and handle it in a foreign country.

GDPR	APPI
Articles 3, 4(1) Recitals 2, 14, 22-25	Articles 75, 86

Similarities

In relation to **extraterritorial scope**, the GDPR applies to organisations that do not have any presence in the EU, but that **offer goods, services or monitor the behaviour of individuals in the EU**.

Article 75 outlines that some provisions of the APPI have an extraterritorial scope, where a business operator, who in **relation to supplying a good or service to a person in Japan**, has acquired personal information relating to a person in Japan and handles it in a foreign country.

Differences

The GDPR also **explicitly applies** to organisations that have a presence in the EU. In particular, under Article 3, the GDPR applies to entities that have an '**establishment**' in the EU, or if the processing of personal data takes place in the context of the activities of that establishment, irrespective of whether the data processing takes place in the EU or not.

The APPI **does not** explicitly mention its applicability for personal information handling business operators established in Japan.

The GDPR does **not** include any enforcement provision directly aimed at a person that committed an offence outside of the EU.

Article 86 **specifies** that criminal fines under Article 82 and 83 of the APPI apply to a person who has committed an offence outside of Japan.

1.3. Material scope

Fairly Inconsistent

The GDPR applies to the processing of personal data, whilst the APPI applies to the handling of personal data for business purposes. Both the GDPR and the APPI apply to personal data and personal information respectively; however, only the APPI the APPI includes anonymously processed information within its scope.

GDPR	APPI
Articles 2, 4(1), 4(2), 4(6) Recitals 15-21, 26	Articles 2, 36, 37

Similarities

The GDPR applies to '**personal data**' which is defined as 'any information that directly or indirectly relates to an identified or identifiable individual' (see section 2.1).

The APPI applies to '**personal information**,' which is defined as 'data relating to a living individual' (see section 2.1). It also defines **personal data** as 'personal information constituting a personal information database.'

The GDPR defines **special categories of personal data** and provides specific requirements for its processing.

The APPI defines **personal information which requires special care** and provides specific requirements for its handling.

The GDPR excludes from its application the processing of personal data by individuals for **purely personal or household purposes** that has 'no connection to a professional or commercial activity.'

The APPI applies to personal information handling business operators which use personal data **in business**.

Differences

The GDPR applies to the **processing** of personal data. The definition of 'processing' covers 'any operation' performed on personal data 'such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'

The APPI does **not** define what activities form part of the handling of personal information. It clarifies that the APPI applies to personal information, retained personal data, and a 'personal information database,' which is defined as 'a collective body of information comprising personal information.'

Anonymous data is specifically outside the scope of the GDPR. Anonymous data is information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The APPI applies to **business operators who handle anonymously processed information**. A business operator must process anonymous data in accordance with standards prescribed by the PPC. '**Anonymously processed information**' under the APPI is defined as information relating to an individual

GDPR	APPI

Differences (cont'd)

	that can be produced from processing personal information, so as neither to be able to identify a specific individual by taking action 'such as deleting part of the identification codes or part of the description included in the personal data.
The GDPR does **not** differentiate between personal data and retained personal data.	Some provisions of the APPI specifically apply to '**retained personal data**,' which is defined as 'personal data which a personal information handling business operator has the authority to disclose, correct, add, or delete the contents of, cease utilisation of, erase, and cease the third party provision of personal data, and which shall be neither those prescribed by a Cabinet Order as likely to harm the public or other interests if their presence or absence is made known, nor those set to be deleted within six months.'

2. Key definitions

2.1. Personal data (personal information)

Both the GDPR and the APPI include a definition of 'personal data' and 'personal information' respectively. Additionally, the APPI defines 'personal data' with regard to personal information databases and 'retained personal data' with regard to the authority to disclose etc. personal data.

The GDPR provides a definition of special categories of personal data and prohibits processing unless one of the exemptions apply. Under the APPI, special care-required personal information cannot be collected and provided to a third party by the opt-out method, except where the principal gives their consent or when exemptions apply.

The APPI applies to anonymously processed information, whereas the GDPR explicitly excludes anonymised data from its scope of application.

GDPR	APPI
Articles 4(1), 9 Recitals 26-30	Articles 2, 17(2)

Similarities

'**Personal data**' is defined as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.' The GDPR also explains in its recitals that in order to determine whether a person is identifiable, 'account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person' to identify the individual directly or indirectly. In its recitals, the GDPR specifies that **online identifiers** may be considered as personal data, such as **IP addresses, cookie identifiers, and radio frequency identification tags.**

'**Personal information**' means 'information relating to a living individual which falls under any of the following: a name, date of birth, or other type of descriptions (meaning any and all matters stated, recorded or otherwise expressed using voice, movement, or other methods in a document, drawing or electromagnetic record (meaning an electronic, magnetic, or other forms of record that cannot be recognised through the human senses)), **whereby a specific individual can be identified** (including those which can be readily collated with other information and thereby identify a specific individual). The same applies for an individual **identification code**, which includes 'any character, letter, number, symbol, or other codes falling under any of the following: identifying a specific individual through a character, letter, number, symbol, or other codes for use with computers converted from a person's bodily information which may identify the person or character, letter, number, symbol, or other codes which are assigned in regard to the use of services provided to an individual or to the purchase of goods sold to an individual, or which are stated or electromagnetically recorded in a card or other document issued to an individual so as to be able to identify a specific user or purchaser, or recipient of issuance by having made said codes differently assigned or, stated or recoded for the user or purchaser, or recipient of

GDPR	APPI

Similarities (cont'd)

	issuance.' The APPI also defines **personal data** as personal information constituting a **personal information database**.
The GDPR defines special categories of personal data as data revealing a data subject's 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'	The APPI also defines **special-care personal information** as information about a principal's 'race, creed social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. prescribed by cabinet order as those of which the handling requires special care so as not to cause unfair discrimination, prejudice or other disadvantages to the principal.'

Differences

The GDPR does **not** apply to '**anonymised**' data, where the data can no longer be used to identify the data subject.	The APPI applies to **anonymously processed information,** which is information that relates to an individual that can be produced from processing personal information so as to neither be able to identify a specific individual nor be able to restore the personal information of that individual. For personal information, this requires deleting part of the descriptions of the data, and in the case of identification codes, to delete them entirely and replace them with other descriptions.
The GDPR does **not** define retained personal data.	The APPI makes reference to **retained personal data**, which a business operator has the authority to disclose, correct, add or delete the contents of, as well as cease utilisation, erase and cease the third party provision of such data.

2.2. Pseudonymisation

The GDPR defines pseudonymised data and clarifies that such data is subject to the obligations of the GDPR. The APPI does not currently define nor regulate pseudonymised data. The concept of pseudonymously processed information is however, newly added under the 2020 Amendment.

Under the 2020 Amendment, 'pseudonymously processed information' is defined as being data about an individual that is pseudonymised by processing personal data so that a specific subject cannot be identified unless it is matched with other data. When a PIC processes pseudonymously processed information, the rule of restriction on changing the utilisation purpose is not applied, and the PIC can change the utilisation purpose without restriction as long as it is for internal use. Therefore, pseudonymously processed information is considered to be a type of information for data utilisation.

GDPR	APPI
Articles 4(5), 11 Recitals 26, 28	Not applicable

Similarities

The GDPR provides a **definition** of pseudonymised data and clarifies that such data is **subject to the obligations of the GDPR**. Notably, **pseudonymised data** is 'personal data that can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.' The GDPR also includes a definition of **anonymised data** (see section 2.1., above).

The APPI **does not currently define pseudonymised data**. The concept of pseudonymously processed information is; however, newly added under the 2020 Amendment.

Differences

Not applicable.

Not applicable.

2.3. Controllers and processors (personal information handling business operators)


Fairly inconsistent

Unlike the GDPR, the concepts of data controller and data processor are not individually defined in the APPI. Instead, the APPI, defines a PIC, which is a person 'providing a personal information database etc. for use in business.'

The GDPR sets out detailed requirements in relation to the processing of personal data by data controllers and data processors. The APPI establishes a number of specific obligations for PICs in relation to the utilisation of a principal's personal information.

GDPR	APPI
Articles 4, 17, 28, 30, 32, 33, 35, 37, 38 Recitals 90, 93	Articles 2, 15, 18, 19, 20, 21, 22, 23, 25, 28, 29, 30, 34, 35

Similarities

Data controllers must comply with the request for the **exercise of data subject rights**, such as the right to erasure, the right to rectification, the right to access, etc. unless exemptions apply. Data processors must comply with data subject's rights if required by the controller.

PICs must respond to a **principal's demand** for notification of utilisation purposes, disclosure, correction, addition or deletion, cessation of utilisation and third-party provision of retained personal data, etc. in cases specified by the law.

Data controllers must comply with the **purpose limitation and accuracy principles**, and rectify a data subject's personal data if it is inaccurate or incomplete.

PICs must ensure that **personal data is accurate and up to date** within the scope necessary to achieve the utilisation purpose and correct, add, or delete any retained personal data of the principal's that is not factual.

Data controllers must implement **technical and organisational security measures**.

Personal information handling business operators must take necessary and appropriate action for the **security of personal data** including **preventing the leakage, loss or damage of the personal data it handles**.

Differences

A **data controller** is a natural or legal person, public authority agency or other body that determines the **purposes** and **means** of the processing of personal data, alone or jointly with others.

There is **no definition for data controller** or data processor under the APPI. A **PIC** is 'a person providing a personal information database etc. for use in business, 'however, the APPI states that central government organisations, local governments, incorporated administrative agencies, and local incorporated administrative agencies are **excluded** from the definition of 'PIC.' In addition, the following are **out of the scope of obligations for PICs under the APPI**: broadcasting institutions,

GDPR	APPI
Differences cont'd	
	newspaper publishers, communication agencies, press organisations, a person who practices writing as a profession, universities, and other organisations aimed at academic studies, as well as political and religious bodies (see Article 76).
A **data processor** is a natural or legal person, public authority, agency or other body which processes personal data on **behalf** of the controller.	There is **no definition of a data processor** under the APPI.
Other obligations are also imposed on processors, such as: **Keeping records of data processing activities**: processors are required to maintain a record of data processing activities in certain situations, including if the processor has 250 or more employees or if it processes data that is likely to result in a risk to the rights and freedoms of data subjects. The record should contain the categories of processing and any data transfers outside of the European Economic Area. **Implementing appropriate technical and organisational measures**: processors must ensure security for processing data, which can include encryption or pseudonymisation practices. **Data Protection Impact Assessments ('DPIA')**: processors should assist the controller to undertake data protection impact assessments prior to processing. **Appointing a Data Protection Officer ('DPO')**: processors must designate a DPO when required by the law, including where a processor processes personal data on a large scale. **Notifying the controller of any data breach**: processors are required to notify controllers of any breach without undue delay after becoming aware of a breach.	Other obligations imposed on personal business operators include: **deleting personal data without delay when such utilisation has become unnecessary**; exercise necessary and appropriate **supervision over an employee and an entrusted person so as to seek the security control of the personal data** of which the handling has been entrusted; **disclose retained personal data to a principal** without delay **pursuant to a method prescribed by a cabinet order**, unless disclosing data falls under Articles 28(2)(i) to (iii); **aim to handle appropriately and properly complaints** about the handling of personal information, and **aim to establish a system necessary to achieve such a purpose** under Article 35(1).

2.4. Children

The GDPR sets specific provisions for protecting children's personal data, in particular, when such data is processed for the provision of information society services. By contrast, the APPI does not include specific provisions on the processing of children's personal information.

GDPR	APPI
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	Articles 16, 17, 23

Similarities

The GDPR does **not** define 'child' or 'children.'

The APPI does **not** define 'child' or 'children.'

Differences

The GDPR considers children as '**vulnerable natural persons**' that merit specific protection with regard to their personal data. In particular, specific protection should be given when children's personal data is used for marketing or collected for information society services offered directly to a child.

The APPI does **not** provide children with special protection with regard to the processing of their personal data. However, the General Rules Guideline states that, in the case where children do not have the capacity to judge the consequences of consenting to the processing of their personal data, it is necessary to obtain consent from their legal representatives such as parents. The Q&A of the APPI also states that PICs are generally required to obtain the consent from their legal representatives such as parents for children under the age of 15.

Where the processing is based on consent, the consent of a parent or guardian is required for providing information society services to a child below the **age of 16**. EU Member States can **lower this age limit to 13**. Data controllers are required to make reasonable efforts to verify that consent is given or authorised by a parent or guardian.

The APPI does **not** list specific conditions to process children's personal information.

The GDPR does not provide for any exception for a controller that is **not aware** that it provides services to a child. It is not clear whether the consent requirement will apply if the child's personal data is unintentionally collected online. 'Fostering healthy children' is not an exemption for obtaining consent.

The APPI states **some exemptions to the need of obtaining consent for each processing**. Such exemptions are (i) cases based on laws and regulations, (ii) cases in which there is a need to protect a human life, body or property, and when it is difficult to obtain a principal's consent, (iii) cases in which there is a special need to enhance public hygiene or promote fostering healthy children, and when it is difficult to obtain a principal's consent, or (iv) cases in which there is a need to cooperate in regard to a central government organisation or a local government, or a person entrusted by them to perform affairs prescribed by the laws and regulations, and when

GDPR	APPI

Differences cont'd

	there is a possibility that obtaining a principal's consent. would interfere with the performance of said affairs.
When any information is addressed specifically to a child, controllers must take **appropriate measures** to provide **information** relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language, that the child can easily understand.	There are **no** specific rules for privacy notices aimed at children.

2.5. Research

The GDPR has specific provisions addressing the processing of personal data for 'historical or scientific research,' as well as for 'statistical purposes.' On the contrary, the APPI does not make any specific reference to the processing of personal information for research purposes.

GDPR	APPI
Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 89 Recitals 33, 159, 160, 161	Article 76 (1) (iii)

Similarities

Not applicable	Not applicable

Differences

Under the GDPR, the processing of personal data for research purposes is subject to some **specific rules** (e.g. with regard to the purpose limitation principle, the processing of special categories of personal data, etc.)	The APPI does **not** include any specific provision for the processing of personal information for research purposes. University and other research groups aimed at academic studies are, though, excluded from its scope of application.

3. Legal basis

The GDPR provides that the processing of personal data will only be lawful where certain grounds are fulfilled (as listed in Article 6 for personal data and Article 9 for special categories of personal data).

The APPI does not provide a general list of legal grounds that need to be met when handling personal information. However, the APPI provides that consent is required in circumstances specified by the law.

GDPR	APPI
Articles 5-10 Recitals 39-48	Articles 16, 17, 23, 24

Similarities

The GDPR recognises **consent** as a legal basis to process personal data.

The APPI recognises that **consent** is necessary with regard to specific circumstances.

Differences

The GDPR states that data controllers can only process personal data when there is a legal ground for it. The legal grounds are: **consent**, or when processing is necessary for (i) the **performance of a contract** which the data subject is part of in order to take steps at the request of the data subject prior to the entering into a contract; (ii) compliance with **legal obligations** to which the data controller is subject; (iii) to protect the **vital interest** of the data subject or of another natural person; (iv) performance carried out in the public interest or in the official authority vested in the data controller; or (v) for the **legitimate interest** of the data controller when this does not override the fundamental rights of the data subject. Further permissible uses are provided for the processing of **special categories of personal data** under Article 9(2). As a general rule, the processing of special categories of personal data is restricted unless an exemption applies, which include the data subject's explicit consent.

The APPI does **not** list the legal grounds that personal information handling business operators must adhere to *a priori* when handling personal data. **Consent** (unless exceptions apply) of the principal is required when (i) the handling goes **beyond the utilisation purpose** already declared to the individual; (ii) personal information is obtained by **another operator as a result of a merger or another reason and the data is used for a different purpose** from the one already specified to the principal; (iii) the personal information **collected is special care-required personal data**; (iv) personal information is **provided to a third party**; and (v) in the context of **cross border data transfers**.

The GDPR includes **specific information** on how consent must be obtained and can be withdrawn, as well as the **elements that make consent valid**.

The APPI does **not** include a definition of consent and it does not specify what elements make consent valid. However, the General Rules Guideline mentions that 'consent of the principal' means an indication of the principal's intention to consent to the handling of his/her personal information in the manner indicated by PICs.

4. Controller and processor obligations

4.1. Data transfers

Fairly inconsistent

Both the GDPR and APPI regulate the cross-border transfer of personal data to third parties and allow such transfers to be performed based on an adequate or equivalent level of protection, respectively. The two jurisdictions also provide that, in the absence of an equivalent level of protection determination, cross border transfers can be undertaken based on consent, as well as other bases. The GDPR, however, outlines a number of appropriate safeguards which allow personal information to be transferred, whereas the APPI allows transfers based on standards prescribed by the PPC. Further to this, the PPC does not address transfers based on international agreements for judicial cooperation, or transfers from registers.

Under the 2020 Amendment, when personal data is provided to a third party in a foreign country based on the consent of the individual, the following information must be provided to the data subject in advance of such consent:

- the details of the personal information protection system of the relevant foreign country;
- the measures to be taken by the third party to protect the personal information; and
- other information that may be helpful to the individual.

In addition, under the 2020 Amendment, personal data may be provided to a third party based on the reason that it has taken measures equivalent to those required to be taken by a PIC under the APPI; namely, it has taken the following measures:

- taking necessary measures to ensure that the third party continues to implement the equivalent measures; and
- providing information on such necessary measures upon the request of the individual.

GDPR Articles 44-50 Recitals 101, 112	APPI Articles 23 and 24
Similarities	
The GDPR allows personal data to be transferred to a third country or international organisation that has an **adequate level of protection** as determined by the EU Commission.	The APPI permits personal information transfers to foreign countries that have been recognised by the PPC as establishing a personal information protection system which provides an **equivalent standard** to that in Japan in regard to the protection of an individual's rights and interests.
One of the following **legal grounds** can be applied to the transfer of personal data abroad: • prior **consent** • when a data subject has explicitly **consented** to the proposed transfer and acknowledged the possible risks of such transfer due to inadequate safeguards;	The APPI provides that consent is generally required for the transferring of personal information to foreign countries. However, personal information can also be transferred on one of the following **bases**: • cases based on **laws and regulations**; • cases in which there is a need to protect a

Similarities (cont'd)

- when the transfer is necessary for the performance or conclusion of a **contract**;
- when the transfer is necessary for important **public interest** reasons;
- when the transfer is necessary for the establishment, exercise, or defence of a **legal** claim; and
- when the transfer is necessary to protect the **vital interests** of a data subject or other persons.

- human life, body, or fortune, and when it is difficult to obtain a principal's **consent**;
- cases in which there is a special need to enhance **public hygiene** or promote fostering healthy children, and when it is difficult to obtain a principal's consent; and
- cases in which there is a need to cooperate in regard to a central government organisation or a local government, or a person entrusted by them performing affairs prescribed by laws and regulations, and when there is a possibility that obtaining a principal's consent would interfere with the **performance of affairs**.

Differences

In the absence of a decision on adequate level of protection, a transfer is permitted when **the data controller or data processor provides appropriate safeguards** with effective legal remedies that ensure the data subjects' rights as prescribed under the GDPR. **Appropriate safeguards include**:

- **binding corporate rules** with specific requirements (e.g. a legal basis for processing, a retention period, complaint procedures, etc.);
- **standard data protection clauses** adopted by the EU Commission or by a supervisory authority;
- an **approved code of conduct**; or
- an **approved certification**.

The APPI **does not** outline appropriate safeguards for the foreign transfer of personal data in the absence of recognised equivalent standards. However, the APPI establishes that cross border transfers can be undertaken where a person establishes a system conforming to standards prescribed by rules of the PPC as necessary to continuously take when transferring personal data to a foreign country.

The GDPR specifies that a cross-border transfer is allowed based on **international agreements** for judicial cooperation.

The APPI makes **no specific reference** to cross-border transfers based on international agreements for judicial cooperation. However, Japan is a member of Asia-Pacific Economic Cooperation Cross-Border Privacy Rules ('APEC CBPRs') which allows PICs to transfer personal information to foreign countries certified under the rules.

The grounds for a cross-border **transfer includes the transfer being made from a register** which, according to the Union or a Member States' law, is intended to provide information to the public, and which is open to consultation either by the public in general or by any person who can demonstrate a **legitimate interest**, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

The APPI **does not** include a similar provision.

4.2. Data processing records

Neither the GDPR nor APPI provide a general requirement for registering with supervisory authorities. In addition, both legislations outline recording keeping requirements in relation to cross border data transfers. On the other hand, the GDPR requires data controllers and processors to maintain a general record of processing activities, whereas the APPI does not impose specific record-keeping obligations on PIC in relation to processing activities.

GDPR Article 30 Recital 82	APPI Article 25

Similarities

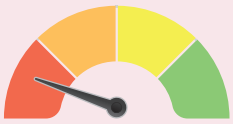
The GDPR **does not** provide general requirements for registering with a supervisory authority.	The APPI **does not** contain general requirements for registering with the PPC.
The GDPR **prescribes a list of information that a data controller** must record regarding **international transfers** of personal data, namely the identification of the third countries or international organisations, and the documentation of adopted suitable safeguards.	The APPI stipulates that PICs must **keep a record** pursuant to rules of the PPC on the date of the personal data transfer, the name or appellation of the third party, and other matters prescribed by rules of the PPC, except where exceptions apply.

Differences

Data controllers and data processors have an obligation to **maintain a record** of processing activities under their responsibility.	The APPI **does not** contain a general requirement for PICs to maintain records of processing activities under their responsibility. However, the General Rules Guideline states that a PIC shall take 'establishment of means for checking the processing status of personal data' as part of the safety management measures.
The GDPR **prescribes a list of information that a data controller** must record: • the name and contact details of the **data controller**; • the **purposes of the processing**; • a description of the categories of **personal data**; • the categories of recipients to whom the personal data will be **disclosed**; • the **estimated period for erasure** of the categories of data; and • a general description of the technical and organisational **security measures** that have been adopted.	The APPI **does not** contain an equivalent provision. However, the General Rules Guideline cites a method of clarifying the following items in advance as an example of 'establishment of means for checking the processing status of personal data': • types and names of personal information databases etc.; • items that include personal data; • responsible person/department; • purpose of utilisation; and • those who have access rights etc.
The obligations in relation to data processing records are also imposed on the **representatives of data controllers**. •	The APPI **does not** contain an equivalent provision.

GDPR	APPI
Differences cont'd	
The processing of information recorded by a data controller shall be in **writing or electronic form**.	The APPI **does not** contain an equivalent provision.
The requirements around data processing records shall not apply to **an organisation with less than 250 employees**, unless the processing: • is likely to result in a risk to the rights and freedoms of data subjects; • is not occasional; or • includes special categories of data in Article 9(1) (e.g. religious beliefs, ethnic origin, etc.) or is personal data relating to criminal convictions and offences in Article 10.	The APPI **does not** contain an equivalent provision. However, the General Rules Guideline shows examples for PICs with 100 or less employees, in addition to the examples for PICs in general.
The GDPR **prescribes a list of information that a data processor** must record: • the name and contact details of the data processor; • the categories of processing carried out on behalf of each controller; • international transfers of personal data, with the identification of third countries or international organisations, and the documentation of adopted suitable safeguards; and • a general description of the technical and organisational security measures that have been adopted.	The APPI **does not** contain an equivalent provision.

4.3. Data protection impact assessment



Inconsistent

The GDPR provides that a Data Protection Impact Assessment ('DPIA') must be conducted under specified circumstances and makes no distinction between private or public entities. The APPI conversely, only requires public institutions to conduct Privacy Impact Assessments ('PIA') in regard to specific personal information files.

GDPR	APPI
Article 35, 36 Recitals 75, 84, 89-93	Article 61(5) Article 27 of the Act on the Use of Numbers to Identify a Specific Individual in Administrative Procedures ('the Use of Numbers Act')

Similarities

Not applicable.	Not applicable.

Differences

A data controller is required to, **where necessary**, carry out a review to assess whether the processing of personal data is in accordance with the DPIA, **particularly when there is a change** in risks to processing operations.

The GDPR provides that a DPIA must be conducted if a data controller utilises **new technologies** to process personal data.

The GDPR provides that a DPIA must be conducted **under the following circumstances**:

- the processing may result in a high risk to the rights and freedoms of an individual;
- when a systematic and extensive evaluation of personal aspects relating to natural persons is involved, which is based on automated processing or profiling;
- there is processing on a large scale of special categories of data; and
- there is systematic monitoring of a publicly accessible area on a large scale.

The APPI **does not** contain PIAs requirements for data processing by PICs. The Use of Numbers Act, however, requires certain administrative and government agencies to conduct PIA's in specified circumstances.

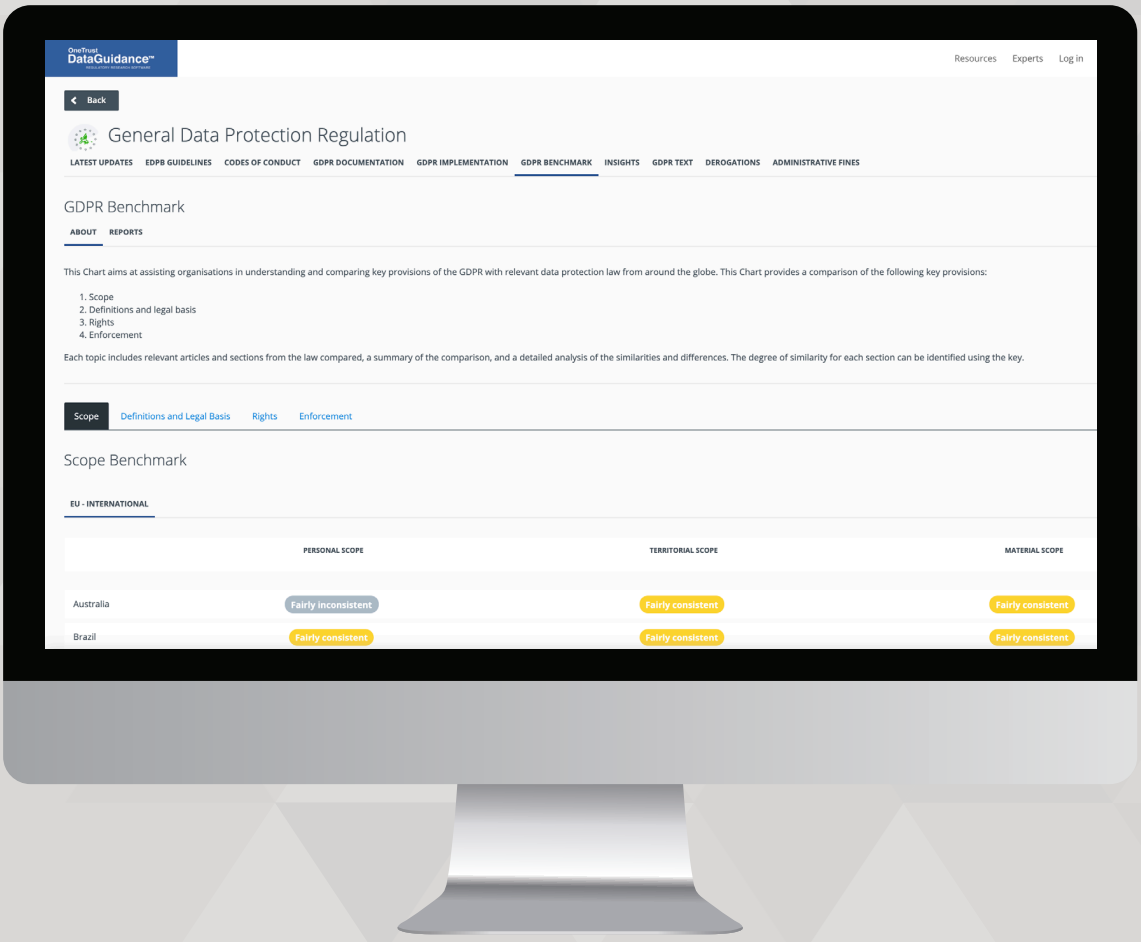
Under the APPI, **only** government and administrative agencies are required to conduct a PIA.

Under the APPI, **only** government and administrative agencies are required to conduct a PIA.

Global Regulatory Research Software

40 In-House Legal Researchers, 500 Lawyers Across 300 Jurisdictions

Monitor regulatory developments, mitigate risk, and achieve global compliance



OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan | China
and 20+ other global laws & frameworks

Understand and compare key provisions of the GDPR with relivant data protection laws from around the globe

The GDPR Benchmarking tool provides comparison of the various pieces of legislation on the following key provisions


Scope


Rights


Definitions and legal basis


Enforcement

- Employ topic specific guidance to develop your compliance activities
- Monitor news and access written opinion pieces on the most recent developments

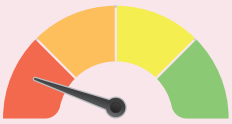
Start your free trial at
www.dataguidance.com

GDPR	APPI

Differences cont'd

The assessment **must contain at least** the following: • a systematic description of the envisaged processing; • operations and legitimate purposes of the processing; • the necessity and proportionality of the • operations in relation to the purposes; and • the risks to the rights and freedoms of data subjects.	Under the APPI, **only** government and administrative agencies are required to conduct a PIA.
A data controller **must consult** the supervisory authority prior to any processing that would result in a high risk in the absence of risk mitigation measures as indicated by the DPIA.	Under the APPI, **only** government and administrative agencies are required to conduct a PIA.

4.4. Data protection officer appointment



Inconsistent

Unlike the GDPR, the APPI does not require data controllers and processors to appoint a DPO in specified circumstances. However, the General Rules Guidelines stipulate the appointment of a person in charge of personal information management as an example of security management measures under the APPI.

GDPR Articles 13 - 14, 37-39 Recital 97	APPI
Similarities	
Not applicable.	Not applicable.
Differences	
The data controller and the data processor shall **designate** a DPO in any case where: • the processing is **carried out by a public authority** or body, except for courts acting int heir judicial capacity; • the core activities of a data controller or data process or consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require **regular and systematic monitoring** of data subjects on a large scale; or • the core activities of the controller or the processor relate to a large scale of **special categories of personal data** (e.g. religious beliefs, ethnic origin, data required for the establishment, exercise, or defence of legal claims etc.)	The APPI **does not** include a requirement to appoint a DPO. However, the General Rules Guidelines outline that security measures must be taken for the handling of personal information, the appointment of a person in charge of the handling of personal information and the definition of the responsibilities of that person, being an example of such security measures.
A group may appoint a **single DPO** who must be easily contactable by each establishment.	The APPI **does not** include a requirement to appoint a DPO.
The DPO shall perform a list of tasks including: • **to inform and advise** the controller or the data processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions; • **to monitor** compliance with the GDPR with other Union or Member State data protection provisions and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; and	The APPI **does not** include a requirement to appoint a DPO.

GDPR	APPI
Differences cont'd	
to act as a contact point the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.	
The DPO shall be designated on the basis of **professional qualities and expert knowledge** of data protection law and practices.	The APPI **does not** include a requirement to appoint a DPO.
The DPO can be a **staff member** of the data controller or data processor, or can perform tasks based on a **service contract**.	The APPI **does not** include a requirement to appoint a DPO.
Contact details of the DPO must be included in the privacy notice for data subjects, and they must be communicated to the supervisory authority.	The APPI **does not** include a requirement to appoint a DPO.
Data subjects **may contact** the DPO with regard to the processing of their personal data as well as the exercising of their rights.	The APPI **does not** include a requirement to appoint a DPO.
The DPO must be **provided with the resources** necessary to carry out his or her obligations under the GDPR.	The APPI **does not** include a requirement to appoint a DPO.

4.5. Data security and data breaches

Inconsistent

In contrast to the GDPR, the APPI does not legally stipulate responses to a personal data breach; however, PPC Notification No. 1 of 2015 (the 'PPC Notification') stipulates that a PIC shall endeavour to report to the PPC, etc. and notify the principal in the event of any leakage, loss, or damage (collectively leakage etc.) of personal data. In addition, there will be a legal obligation to report any leakage etc. to the PPC and notify the principal under the 2020 Amendment.

GDPR	APPI
Article 5, 24, 32-34 Recitals 74-77, 83-88	Article 20 PPC Notification

Similarities

The GDPR recognises **integrity** and **confidentiality as fundamental principles** of protection by stating that personal data must be processed in a manner that ensures appropriate security of the personal data.

The APPI states that a PIC shall take necessary and appropriate action for the **security control** of personal data including preventing any leakage etc. of its handled personal data.

In the case of a personal data breach, the data controller must notify the competent supervisory authority of the breach, unless the personal data breach is unlikely to result in a risk to the individuals' rights and freedoms.

According to the PPC Notification, when a case of leakage etc. is discovered, a PIC shall endeavour to promptly **report certain matters to the PPC** regarding the facts of the case and measures to prevent recurrence.

The controller must notify **the** data subject of a data breach without undue delay if the data breach is likely to result in a high risk to the rights and freedoms of natural persons.

According to the PPC Notification, the PIC shall, depending on the contents of the leakage etc., promptly **inform the person in question** of the facts or make them readily available to the person in question, from the viewpoint of preventing secondary damage and the occurrence of similar cases.

Differences

Under the GDPR, the obligation of data controllers to notify data subjects when the data breach is likely to result in a high risk to the rights and freedoms of natural persons, is exempted in certain circumstances such as where:

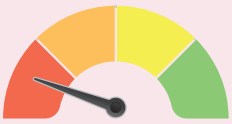
- **appropriate technical and organisational protective measures** have been implemented;
- any **subsequent measures** have been taken in order to ensure that the risks are no longer likely to materialise; or
- it would involve **disproportionate effort**.

The PPC Notification states that a PIC is **not** required to report to PPCs in any of the following cases:

- when it is judged that personal data has not been substantially leaked to outside parties; and
- in the case of minor misdirection of a fax or e-mail, or misdelivery of a package, etc.

GDPR	APPI
Differences cont'd	
Under the GDPR, a personal data breach must be notified to the supervisory authority **without undue delay** and, where feasible, **no later than 72 hours** after having become aware of the breach.	The APPI and the PPC Notification **do not** include an equivalent provision . However, the PPC Notification does recommend that PICs should endeavour to **promptly report** the facts and measures to prevent recurrence to the PPC in certain circumstances.
The GDPR **provides a list of information** that must be, at minimum, **included in the notification** of a personal data breach. For example, a notification must describe the nature of the breach, the approximate number of data subjects concerned, and the consequences of the breach.	The APPI and the PPC Notification **do not** include an equivalent provision.
The GDPR provides a **list of technical and organisational measures**, where appropriate, that data controllers and data processors may implement such as pseudonymisation, encryption and the ability to restore availability and access to personal data in a timely manner in the event of physical or technical incidents, to ensure integrity and confidentiality.	The APPI and the notification **do not** include an equivalent provision.
The GDPR states that data processors must notify **the data controller** without undue delay after becoming aware of the personal data breach.	The APPI and the notification **do not** include an equivalent provision.

4.6. Accountability



Inconsistent

Unlike the GDPR, the APPI does not explicitly refer to the concept of accountability, however, the APPI does contain provisions that can be taken to apply to accountability including the requirement to keep records in specific circumstances.

GDPR Articles 5, 24-25, 35, 37 Recital 39	APPI

Similarities

GDPR	APPI
Not applicable.	Not applicable.

Differences

GDPR	APPI
The GDPR recognises **accountability** as a fundamental principle of data protection. Article 5 states that 'the data controller shall be responsible and able to demonstrate compliance with, paragraph 1 [accountability].' In addition, the principles can be taken to apply to several other principles as mentioned in other sections of this report, including the appointment of a DPO, and DPIAs.	The APPI **does not** explicitly refer to the term accountability. However, the APPI does contain provisions related to accountability including the requirement to maintain records in relation to third-party-provisions of personal data, unless exceptions apply.

5. Rights

5.1. Right to erasure (right to cancellation)

Fairly inconsistent

Both the GDPR and the APPI allow individuals to request the deletion of their personal information unless exceptions apply. The exceptions, scope, and applicability vary between the two laws. However, under the 2020 Amendment, the APPI allows a principal to request the deletion of use of retained personal data in the following cases:

- when there is no longer a need to use the retained personal data;
- when a leak or other situation occurs; and
- when there is a risk of harm to the rights or legitimate interests of the principal.

GDPR	APPI
Articles 12, 17 Recitals 59, 65-66	Articles 19, 29, 30, 32(4), 33

Similarities

The **right to erasure** only applies if either of the following grounds are met: where consent is withdrawn and there is no other legal ground for processing, or when personal data is no longer necessary for the purpose for which it was collected. The scope of this right is not limited to the data controller, but also impacts **third parties**, such as recipients, data processors and sub-processors that may have to comply with erasure requests.

When retained personal data of the principal is handled in violation of the provisions of **Article 16**, or is acquired in violation of the provisions of **Article 17**, the principal can demand the deletion of their personal information. Deletion may also be requested when information about the principal is not factually correct.

This right can be exercised **free of charge**. However, there may be some instances where a fee may be requested, notably when the requests are unfounded, excessive, or have a repetitive character.

This right can be exercised free of charge, with no exceptions set forth in the APPI.

Differences

Among the exceptions to the right of erasure provided by the GDPR are: **freedom of expression** (free speech), freedom of information; processing for **research purposes** of personal data that, if erased, would impair the objectives of the research; **establishment, exercise or defence of legal claims**; and for **complying with a legal obligation**. A data controller is also exempted from complying with erasure requests for reasons of **public interest in the area of public health**.

Exceptions to deletion include; in cases where deletion of the retained personal data requires a **large amount of expenses** or other cases where it is difficult to fulfil deletion and when **necessary alternative action** is taken to protect a principal's rights and interests.

Methods to submit an erasure request include in **writing, orally and by other means which include electronic means** when

The APPI stipulates that the **PIC may establish a method** for receiving requests or demands from the principal.

GDPR	APPI
Differences (cont'd)	
appropriate. If the controller has made the personal data public, said controller must take 'reasonable steps, including technical measures,' to inform other controllers that are processing the personal data that the data subject has requested the erasure of any links to, or copy or replication of, those personal data.	In this case, the principal shall make a request for deletion in accordance with the relevant method.
The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is to be deleted.	The APPI **does not** address the mechanisms for PICs to ensure that requests are made by the principal.
Data subjects **must be informed** that they are entitled to ask for their data to be erased.	The APPI **does not** make reference as to whether principals must be informed of their right to request the cancellation of their personal data.
Data subjects' requests under this right must be replied to without 'undue delay and in any event within **one month** from the receipt of the request.' The deadline can be extended to **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.	The APPI requires that PICs shall endeavour to delete personal data without delay when retaining the data is no longer necessary for the stated utilisation purpose for which they collected and held the data. PICs shall endeavour to act '**appropriately and promptly**' when having received such complaints. There is no clarification on the meaning of 'without delay' in the APPI.

5.2. Right to be informed

Both the GDPR and the APPI include provisions relating to the information that organisations must provide to individuals when collecting and processing their personal information.

GDPR	APPI
Articles 5, 12, 13, 14 Recitals 58 - 63	Articles 15, 18, 23, 27

Similarities

The GDPR states that information on the following must be provided to individuals: **identity** of the data controller; the **purposes** of processing; the **existence** of data subjects' rights and the **contact details** of the data protection officer; as well as any **transfer of personal data** to third parties.

The APPI states that information on the following must be provided to the principal: the **name or appellation** of the PIC; the **utilisation purpose** of all retained personal data (unless exemptions apply); the **procedures for responding to a request** in relation to exercise of the principal rights (only when specified) and where to file complaints regarding the handling of retained personal data.

Data controllers **cannot** collect and process personal data for purposes other than the ones about which the consumers were informed, unless they provide them with further information.

PICs must, in case of altering the utilisation purpose, inform the principal of, or disclose to the public, the **altered utilisation purpose**.

The GDPR states that information must be provided to data subjects by controllers at **the time when personal data is obtained**, when the personal data is **collected directly from data subjects**.

The APPI states that PICs must, in cases of having acquired personal data, except where the utilisation purpose has been disclosed in advance to the public, promptly **inform a principal of, or disclose to the public, the utilisation purpose**.

Differences

The GDPR also states that information on the following must be provided to individuals: the categories of personal data processed; the **legitimate interest** of the data controller or the third party; the recipients or **categories** of personal data; transfer of data to third parties; data retention periods; the **right to withdraw consent** at any time; the **right to lodge a complaint** with a supervisory authority; when data is necessary for the performance of a contract, the possible consequences of not providing said data; and the existence of automated decision-making, such as profiling, including the logic involved and consequences of such processing.

In addition, the APPI states that in cases where the PIC acquires a principal's personal information including through a contract, written contract or other document, or similar cases where it acquires directly from a principal his or her personal information stated in a written document, they must state a **utilisation purpose** explicitly to the principal.

GDPR	APPI

Differences

The GDPR provides specific information that must be given to the data subject **when their data is collected by a third party**, which include the sources from which data was collected. **Notice must be given within a reasonable period** after obtaining the data, but at the latest within one month, or at the time of the first communication with the data subject, or when personal data are first disclosed to a recipient.

The APPI **does not explicitly outline transparency** requirements when data is collected indirectly by a third party.

5.3. Right to object (right to cease utilisation)

Both the GDPR and the APPI allow for individuals to exercise their right to object or to cease utilisation respectively and require businesses to provide individuals with information about this right. However, the scope of application of this right under GDPR and APPI differ.

Unlike the GDPR, the APPI does not outline any specific information on the right to object for direct marketing purposes and does not explicitly refer to the right to withdraw consent. However, under the 2020 Amendment, the APPI allows a principal to request the deletion or cessation of use of retained personal data in the following cases:

- when there is no longer a need to use the retained personal data;
- when a leak or other situation occurs; and
- when there is a risk of harm to the rights or legitimate interests of the principal.

GDPR	APPI
Articles 7, 18, 21	Articles 23, 27, 30

Similarities

The GDPR provides data subjects with the **right to object** to the processing of their personal data.

The APPI provides principals with a **right to demand** PICs to cease utilisation of retained personal data that can identify them.

Information about this right and on how to exercise it must be included in the **privacy notice**. In particular, in the context of direct marketing, opting-out must be as easy as opting-in.

PICs are required to make available to the principal, among other things, information about the possibility of utilisation cessation in response to a principal's request, provision to a third party of personal data, and procedures for responding to a request to cease utilisation.

The GDPR states that where requests from a data subject are manifestly **unfounded or excessive**, in particular because of their repetitive character, the controller may either charge a reasonable fee, or refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request

The APPI highlights that the obligation to cease utilisation and delete retained personal data **does not apply** if it requires a large amount of expenses, or in circumstances where it is difficult to fulfil a cease utilisation request and necessary alternative action is taken to protect a principal's rights and interests. A PIC shall endeavour to give an explanation to the principal if the PIC does not fulfil entirely or partially a demand to cease utilisation.

Differences

The GDPR provides that the right to object applies to the processing of personal data when the processing is based on the **legitimate interests** of a data controller or third party. The data controller would have to cease processing personal data unless it demonstrates that there are compelling

The APPI highlights that a principal may request a PIC to **cease utilisation or delete** retained personal data that can identify them if the data was handled in violation of Article 16 or acquired in violation of Article 17 of APPI. In addition, the PIC must stop providing retained personal data to

GDPR	APPI

Differences (cont'd)

legitimate grounds to continue the processing. Moreover, the data subject has the right to object to processing for direct marketing as well as to withdraw consent at any time.	third parties, upon **request** by the principal, if the data was provided in violation of Article 23 (1) or Article 24 of the APPI.
Data subjects have several ways to opt-out of processing of their personal data: they can **withdraw consent**; they can **exercise the general right to object** to processing that is based on legitimate interests or on a task carried out in the public interest; or they **can object to processing of their data for direct marketing purposes**.	The APPI does **not** refer to withdrawing consent for direct marketing purposes.

5.4. Right of access (disclosure)

Both the GDPR and the APPI establish a right of access, which allows individuals to access personal data about them held by organisations.

However, the two laws have notable differences including the instances in which an organisation may refuse an access request. Furthermore, the APPI provides that a fee may be charged when access is granted.

GDPR	APPI
Articles 12, 15, 20 Recitals 59-64	Articles 27, 28, 32, 33

Similarities

The GDPR recognises that data subjects have the **right to access** personal data that a data controller is processing about them.

The APPI recognises that principals have the right to **request a PIC to disclose retained personal data** that can identify them.

Differences

The GDPR states that, when responding to an access request, a data controller must indicate the **purposes** of the processing; the **categories of personal data concerned**; the **recipients or categories of recipients** to whom personal data has been disclosed to; and **any sources** from which data was collected. In addition, the data controller must include further information in the response to a request for access such as the retention period, the right to lodge a complaint with the supervisory authority, the existence of automated decision making, and existence of data transfers. The GDPR specifies that individuals also have the right to receive a **copy** of the personal data processed about them.

The APPI states that a PIC shall disclose retained personal data about the principal, but it **does not** include a prescriptive list of the information a PIC must disclose as part of a disclosure demand. However, the APPI states that the PIC must, when requested by a principal, inform them about the utilisation purpose of retained personal data that can identify them.

Data controllers can **refuse to act** on a request when it is manifestly unfounded, excessive, or has a repetitive character. The GDPR also states, 'That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property, and in particular the copyright protecting software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the data controller processes a large quantity of information concerning the data subject, the data controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.'

PICs may **refuse to disclose data** in cases where disclosing such data would result in the possibility of harming a principal or third party's life, body, fortune, or other rights and interests, seriously interfere with the PIC conducting its business properly, or violate other laws or regulations.

GDPR	APPI

Differences (cont'd)

Data subjects must have a variety of means through which they can make their request, including through **electronic means and orally**. When the request is made through electronic means, the data controller should submit the response through the same means.	The PIC **must disclose personal data pursuant to a method prescribed** by a Cabinet Order. The Cabinet Order stipulates that, when responding to a request for disclosure of retained personal data, in principle, it should be disclosed in writing.
The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is made by the data subject whose personal data is requested access to.	The APPI does not explicitly address **mechanisms** to ensure that the request is made by the principal whose retained personal data is requested access to. However, Article 32(1) of the APPI stipulates that a PIC may establish a method of identity verification as part of the method of exercising the rights of the principal, in which case the principal must follow such method. In addition, Article 32(3) states that a request can be made through an agent pursuant to those prescribed by a Cabinet Order.
The GDPR states that data subjects can exercise this right **free of charge**. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character.	The APPI states that PICs **may collect a fee** which is within a range recognised as reasonable considering the actual expenses when responding to a request only if the fee was specified be the PIC.
Data subjects' requests must be complied with without '**undue delay** and in any event within **one month** from the receipt of the request.' The deadline can be extended to **an additional two months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.	A PIC shall, when requested by a principal to be informed of the utilisation purpose of retained personal data that can identify them, inform the principal **without delay**.

5.5. Right not to be subject to discrimination for the exercise of rights

The right not to be subject to discrimination for the exercise of rights is not explicitly included in either the GDPR or the APPI. However, some provisions based on the same principle can be found in both laws.

GDPR	APPI
Articles 5, 22 Recitals 39, 71-73	Article 3

Similarities

The GDPR does not explicitly include this right and therefore **no scope is defined.**

Although the GDPR does not include an explicit provision stating that a data subject must not be discriminated against on the basis of their choices on how to exercise their data protection rights, it is implicit from the principles of the GDPR that individuals must be protected from discriminatory consequences derived from the processing of their personal data. For example, Article 5 states that personal data must be processed '**fairly**.'

The APPI does not explicitly include this right and therefore **no scope is defined**.

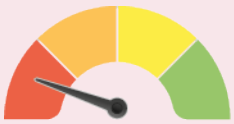
The APPI does not include an explicit provision stating that a principal must not be discriminated against on the basis of their choices on how to exercise their data protection rights. However, it is implicit from its provisions that individuals must be protected against discrimination. For example, Article 3 states that personal information should be **carefully handled** 'under the vision of respecting the personality of an individual.'

Differences

The GDPR also includes some provisions that reflect this principle, such as Article 13 which states that data subjects must be informed of the **consequences derived from automated decision-making**, and Article 22 which specifies that individuals have the **right not to be subject to automated decision-making that has a legal or significant effect upon them**. Additionally, the GDPR emphasises that when processing is based on consent, in order for consent to be valid, it must be freely given and the withdrawal of consent must be without detriment.

The APPI does **not** include any specific provisions directly reflecting this principle.

5.6. Right to data portability



Inconsistent

The GDPR introduced a right to data portability, which allows individuals to obtain the personal data they provided in a structured, commonly usable, and machine-readable format when the processing is based on consent or a contract and is carried out by automated means. The APPI does not address a right to data portability. However, under the 2020 Amendment, the APPI allows a principal to instruct a PIC on the method of disclosure, including disclosure by electromagnetic records, when requesting disclosure from the PIC.

GDPR	APPI
Articles 12, 20 Recital 68	Not applicable

Similarities

Not applicable	Not applicable

Differences

The GDPR **recognises** the right of individuals to obtain their personal data in a structured, commonly usable and machine-readable format when processing is based on consent or contract as well as automated means.	The APPI does **not** recognise a right to data portability.

6. Enforcement

6.1. Monetary penalties

Both the GDPR and the APPI provide for monetary penalties to be issued in case of non-compliance. However, the nature of the penalties differ, it being administrative under the GDPR, and criminal as well as non-criminal under the APPI.

GDPR	APPI
Article 83-84 Recitals 148-152	Articles 82-88

Similarities

The GDPR provides for **monetary penalties i**n case of non-compliance.

The APPI provides for **monetary penalties** in case of non-compliance.

Differences

Administrative fines can be issued by a data protection authority. The administrative fine can be imposed by the competent data protection authority, taking into account that several data protection authorities may be involved if the violation concerns more than one Member State.

Criminal and non-criminal fines can be issued by a Court.

Depending on the violation that has occurred the penalty may be up to either: **2% of global annual turnover or €10 million**, whichever is higher; or **4% of global annual turnover or €20 million**, whichever is higher. The amount of the penalty may also vary depending on 'the nature, gravity and duration of the infringement,' the nature of the processing, the number of data subjects affected and the damages suffered, the negligent or intentional character of the infringement, etc. (A complete list can be found in Article 83(2) of the GDPR.)

Depending on the violation occurred the **criminal penalty** may be up to:

- **JPY 1 million** (approx. €7,600) or imprisonment with work for not more than two years for a person involved in the PPC who has divulgated, or used by stealth, a secret in violation of the provisions of Article 72. Article 86 states that this provision shall apply to a person who has committed an offence outside of Japan.
- **JPY 500,000** (approx. €3,800) or imprisonment with work for not more than one year for a PIC, or its employees or former employees, that have provided, or used by stealth, a personal information database etc. in relation to their business for the purpose of seeking their own or a third party's illegal profit. Article 86 states that this provision shall apply to a person who has committed an offence outside of Japan.
- **JPY 300,000** (approx. €2,300) or imprisonment with labour for not more than six months for a person that has violated an order pursuant to the provisions of Article 42 (2) or (3).
- **JPY 300,000** (approx. €2,300) for a person who has failed to submit a report or material under Article 40(1)

GDPR	APPI

Differences (cont'd)

did falsely respond, or refused, obstructed or evaded an inspection; or failed to submit a report or falsely submit a report under Article 56.

- **Non-criminal fines** up to JPY 100,000 (approx. €750) may be issued to a person that has violated Article 26(2) or Article 55 or has failed to submit a notification or did falsely submit a notification under Article 50(1).

5.2. Supervisory Authority

Fairly consistent

Both the GDPR and the APPI provide for the establishment of an authority with investigatory and corrective powers to supervise the application of the law, and to assist organisations in understanding and complying with it. The GDPR also provides such an authority with the power to impose monetary penalties, while the Personal Information Protection Commission ('PPC') as regulated by the APPI, does not have the power to issue monetary penalties.

In addition, in the EU, national data protection authorities form part of the European Data Protection Board, a body that ensures the consistent application of the GDPR across Europe.

GDPR	APPI
Articles 51 - 84 Recitals 117 - 140	Articles 40 - 46, 59 - 74

Similarities

Data protection authorities have the task to **promote awareness and produce guidance** on the GDPR.	The PPC has the task to **produce guidance and promote the application** of the APPI.
The GDPR states that data protection authorities must act in '**complete independence when performing their tasks**.'	The APPI states that the Chairperson and the Commissioners '**exercise their official authority independently**.'
Data protection authorities have **investigatory powers** which include the capacity to: 'conduct data protection audits, access all personal data necessary for the performance of its tasks, obtain access to any premises of the data controller and processor, including equipment and means.'	The PPC has **investigatory powers**, which include the capacity to demand information, and conduct onsite visits.
Data protection authorities have **corrective powers** which include: 'issuing warnings, reprimands, to order the controller and processor to comply, order the controller to communicate a data breach to the data subject, impose a ban on processing, order the rectification or erasure of data, suspend the transfer of data.'	The PPC has **corrective powers** which include suspending violating actions or taking other necessary actions to rectify violations, as well as providing guidance and advice.
The GDPR does **not regulate how data protection authorities are funded**, this being left to the Member States to decide.	The APPI does **not** include specific provisions establishing how the PPC is funded.

Differences

Data protection authorities **have** the power to impose administrative fines.	The PPC **does not have** the power to directly impose monetary penalties.
The GDPR does **not** include prescriptive rules regarding the internal organisation of each supervisory authority, this is left to Member States to decide.	The APPI specifically **regulates the internal structure** of the PPC, which includes, among other things, provisions on the number of members, their status, and the length of their term.

5.3. Civil remedies for individuals

The GDPR provides individuals with a cause of action to seek damages for privacy violations. The APPI outlines the procedure for when a principal intends to file a lawsuit with regard to rights of disclosure, correction, and utilisation cessation.

GDPR	APPI
Articles 79-82 Recitals 141-147	Articles 34

Similarities

The GDPR provides that data subjects **may bring a claim before the Court** for violations of the GDPR.

The APPI recognises that principals **may file a lawsuit for violations of the APPI**. It specifically addresses scenarios in which a lawsuit is filed in connection with the rights to disclosure, correction, and utilisation cessation.

Differences

The GDPR provides that **any violation of its provisions can trigger a claim for judicial remedies**, and it does not specify the steps data subjects must take before bringing such matters to court. Data subjects can claim **both material and non-material damages**.

The APPI states that a principal may not file a lawsuit in connection with a demand related to the right of the principal, unless 'the principal had previously **issued the demand against a person who should become the defendant in the lawsuit and two weeks have passed from the delivery day of the issued demand**. This, however, shall not apply when the person who should become a defendant in the lawsuit has rejected the demand.'

The GDPR **allows** Member States to provide for the possibility for data subjects to give a mandate for representation to an association or organisation that has as its statutory objective the protection of data subject rights.

The APPI does **not** include any provision **explicitly** recognising the possibility for principals to give a mandate for representation to associations and/or organisations.