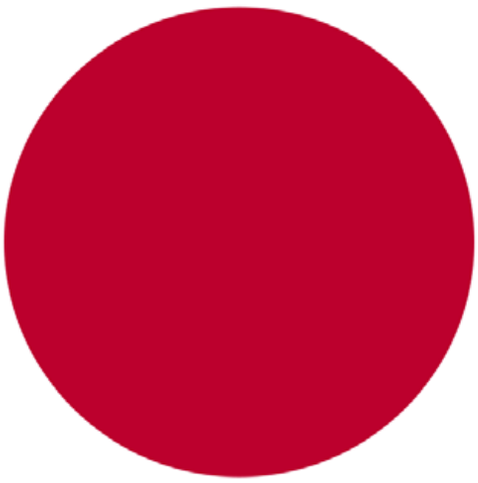


Comparing privacy laws:
GDPR v. APPI

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

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 (e.g. 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™
Alexis Kateifides, Angela Potter, Holly Highams, Claudia Strugnell,
Christopher Campbell, Alice Marini, Angus Young, Victoria Ashcroft

Image production credits:

Cover/p.5/p.39: cnythzl / Signature collection / istockphoto.com
Cover/p.5/p.39: flowgraph / Essentials collection / istockphoto.com
Scale key p6-36: enisaksoy / Signature collection / istockphoto.com
Icon p.12-18: Moto-rama / Essentials collection / istockphoto.com
Icon p.19: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.22-31: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.32-37: cnythzl / Signature collection / istockphoto.com

Table of contents

Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GPDR') and the Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2016) ('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 a revised version came into force on 30 May 2017. One year later, on 25 May 2018, the GDPR entered into force. Discussions regarding an adequacy decision began soon after between the European Commission and the Personal Information Protection Commission of Japan, and the latter started to issue supplementary legislation to enhance its personal data protection. On 23 January 2019, Japan became the first country in Asia to be granted adequacy status by the European Commission. This decision indicated that the APPI, in conjunction with other relevant provisions in Japanese law, provides 'essentially equivalent' protection for personal data as 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 handling business operators. 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, pseudonymised data, 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. €8,225). The APPI does, however, stipulate imprisonment as a potential penalty. Additionally, the APPI applies to anonymised data, while the GDPR explicitly excludes such data.

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.

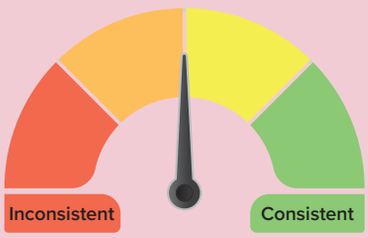
Key for giving the consistency rate

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

Both the GDPR and the APPI protect living individuals with regard to the use of their personal data. The GDPR, though, provides that individuals are protected regardless of their nationality and/or residency, while the APPI does not explicitly address this point.

Furthermore, the GDPR applies to 'data controllers' and 'data processors,' who may be businesses, public bodies, institutions or not for profit organisations. The APPI applies to a 'personal information handling business operator' which is defined as a 'person providing a personal information database etc. for use in business.'

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

Similarities

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.'

Differences

The GDPR applies to a '**data controller**' that is defined by the fact that it establishes the **means** and **purposes of the processing**.

The APPI applies to a '**personal information handling business operator**,' which is defined as 'a person providing a personal information database etc. for use in business.'

The GDPR sets several obligations that apply to '**processors**,' which are entities that process personal data **on behalf of controllers**.

The APPI **only** explicitly refers to 'personal information handling business operators' as being subject to its obligations.

The GDPR applies to businesses, public bodies, institutions and not for profit businesses.

The APPI states that central government organisations, local government, incorporated administrative agencies, and local incorporated administrative agencies are **excluded** from the definition of 'personal information handling business operators.' In addition, the following are **out of the scope of the APPI**: broadcasting institutions, 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 (as specified in Article 76).

GDPR	APPI
Differences (cont'd)	
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.

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 the 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 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

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 applies to anonymously processed data.

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 it 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

The APPI applies to **business operators who handle anonymously processed information**. A business operator must process anonymous data in accordance with

GDPR	APPI
Differences (cont'd)	
personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	standards prescribed by the Personal Information Protection Commission ('PPC'). '**Anonymously processed information**' under the APPI is defined as 'information relating to an individual 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.'

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. In particular, the GDPR provides a definition for sensitive data ('special categories of personal data') and prohibits processing unless one of the exemptions applies; under the APPI, special care-required personal information may be handled 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. Furthermore, the APPI defines 'personal data' with regard to personal information databases and 'retained personal data.'

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 description [...] 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 code falling under any of the following: identifying a specific individual through a character, letter, number, symbol or other code 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 the said codes differently assigned or, stated or recoded for the said user or purchaser, or recipient of issuance.' The APPI also defines **personal data** as personal information constituting a **personal information database**.

GDPR	APPI

Similarities (cont'd)

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.

2.2. Pseudonymisation

The GDPR defines pseudonymised data and clarifies that it is subject to the GDPR obligations. The APPI does not define nor regulate pseudonymised data.

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

Similarities

Not applicable.

Not applicable.

Differences

The GDPR provides a **definition** of pseudonymised data and it 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 are not attributed to an identified or identifiable natural person.' The GDPR also includes a definition of **anonymised data** (see section 2.1.).

The APPI does **not define pseudonymised data.** However, it defines and regulates '**anonymously processed information**' (see section 2.1.).

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

Unlike the GDPR, the concepts of data controller and data processor are not individually defined in the APPI. Instead, the APPI defines a personal information handling business operator, which refers to a person who provides 'a personal information database etc. for use in business.'

The GDPR establishes 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 personal information handling business operators 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, 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.

Personal information handling business operators must respond to a **principal's demand** for utilisation cessation or deletion of retained personal data, etc. in the cases specified by 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.

Personal information handling business operators must ensure that **personal data is accurate and up to date** in order to achieve the utilisation purpose, and correct 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**.

GDPR	APPI
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 either a data controller or data processor under the APPI. A **personal information handling business operator** is 'a person providing a personal information database etc. for use in business'; however, the APPI states that central government organisations, local government, incorporated administrative agencies, and local incorporated administrative agencies are **excluded** from the definition of 'personal information handling business operator.' In addition, the following are **outside the scope of the APPI**: broadcasting institutions, 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**: 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: **delete personal data without delay when utilisation has become unnecessary**; exercise necessary and appropriate **supervision over an entrusted person** so as to ensure 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 28(2)(i) to (iii); **manage appropriately and properly complaints** about the handling of personal information; and **aim to establish a system necessary to achieve such a purpose**.

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.

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 that an **exemption to the need to obtain consent**, which is required only in the cases specified by the law, are '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.'

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.

Fairly inconsistent

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 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) 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 specified already to the individual; (iii) the personal information **handled 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.

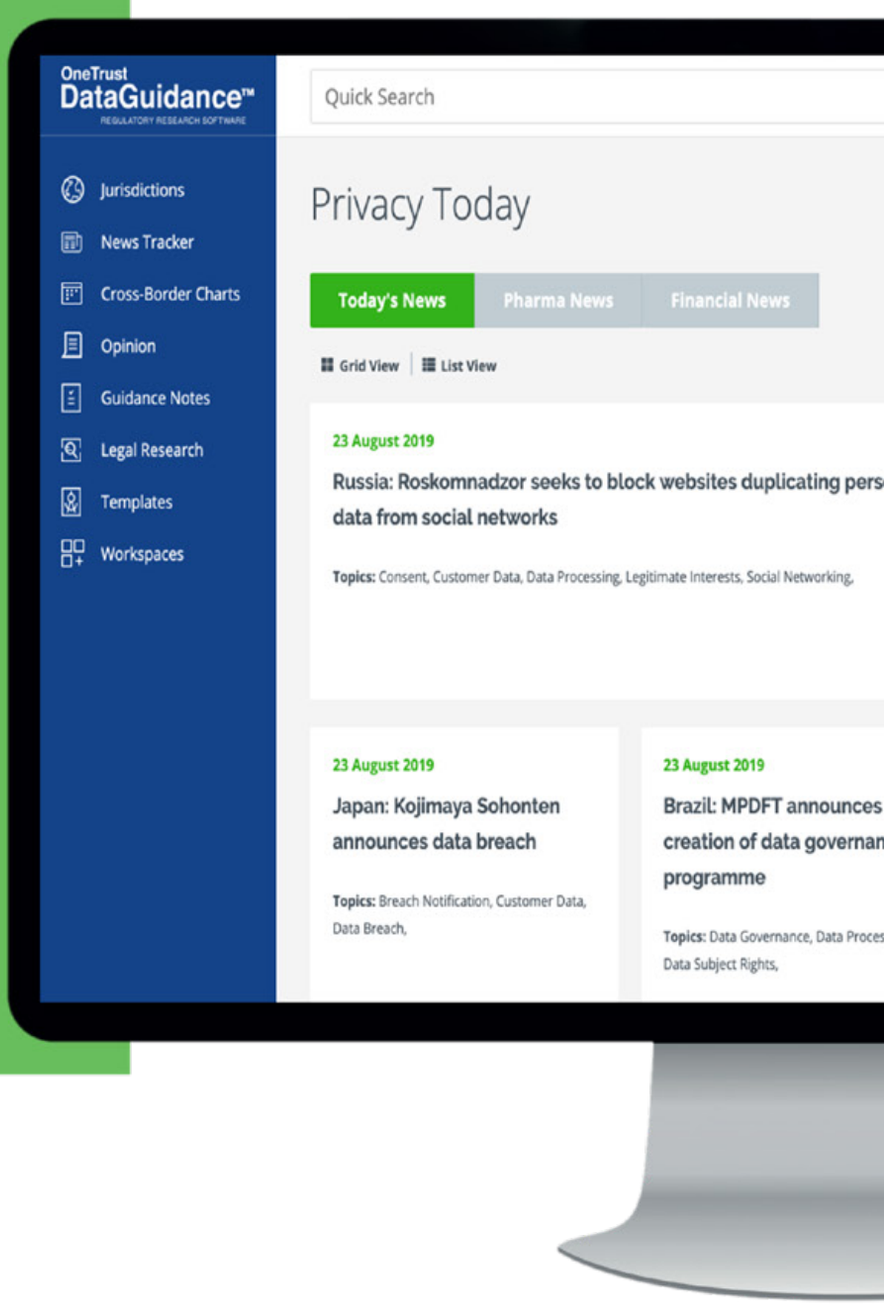
GDPR Portal

The most comprehensive resource for the development and maintenance of your GDPR programme.

- Understand obligations and requirements across key topics and sectors
- Track developments regarding Member State implementation and regulatory guidance
- Apply expert intelligence to make business decisions
- Utilise GDPR specific checklists and templates

OneTrust
DataGui
REGULATORY R

OneTrust DataGuidance is
professionals to monitor r
mitigate risk and achie



4. Individuals' rights

4.1. Right to erasure (right to cancellation)

Both the GDPR and the APPI allow individuals to request the deletion of their personal information. The two laws, however, vary in terms of the scope and applicability of the exceptions they provide regarding the right to erasure.

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.

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 cancellation include: cases based on laws and regulations; cases in which there is a **need to protect a human life**, body or fortune, and 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 it is difficult to obtain a principal's consent; 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 the said affairs. Exemptions in response to a demand for correction are different, and business operators can prevent correction **when discontinuance or erasure costs are significant or otherwise impose hardships on the business operator** and one or more alternative measures to protect the individual's interests are taken.

GDPR	APPI
Differences (cont'd)	
Methods to submit an erasure request include in **writing, orally and by other means which include electronic means** when 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.	The APPI does **not** explicitly address how the request/ demands are practically meant to be completed.
This right can be exercised **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 business operator, when having received a request to inform of a utilisation, can **collect a fee** within a range recognised as reasonable considering the actual expenses.
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 operators 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 business operators 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. Operators must act '**appropriately and promptly**' when having received such complaints. There is no further mention of what 'without delay' means.

4.2. 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 **personal business operator**; the **purpose** of utilising the personal information as explicitly as possible (unless exemptions apply); the **procedures for responding to a request** in relation to exercise of the principal's rights and the **contact information of who handles complaints**. Transfers of data to a third party must be communicated to the principal, unless exemptions apply.

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.

Personal information handling business operators must, when altering a 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 the principal 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**.

GDPR	APPI
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.	The APPI states that in cases where the business operator 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 said principal.
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.

4.3. Right to object (right to cease utilisation)

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

However, the scope of application of this right under the two laws differs. 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.

GDPR Articles 7, 18, 21	APPI 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** that utilisation of the personal information that can identify them ceases.

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.

Business operators 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 information **does not apply** if it requires a large amount of expense, or in circumstances when it is difficult to fulfil a utilisation cessation and when necessary alternative actions are taken to protect the principal's rights and interests. A reason must be given to the principal if a business operator does not fulfil, entirely or partially, a cease utilisation demand.

Differences

With regard to the scope of this right, the GDPR provides that it applies to the processing of personal data when the processing is based on the legitimate interest of the controller or a third party. The data controller would have to cease processing personal data unless they demonstrate that there are compelling, 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.**

With regard to the scope of this right, the APPI highlights that a principal may request a business operator to **cease utilisation, delete** the retained personal information that can identify them and to stop providing the retained personal data to a third party, if the data was handled in violation of Article 16 or acquired in violation of Article 17 of APPI. In addition, the business operator must cease utilisation and delete retained personal data upon **request** by the principal if the request

GDPR	APPI
Differences (cont'd)	
	has **reasonable grounds**. Furthermore, the right to cease utilisation applies in the context of transferring personal data.
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.

4.4. Right of access (disclosure)

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

The two laws, though, differ as to when an organisation may refuse a request. In addition, 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 that a business operator disclose retained personal data** which 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 personal information business operator shall disclose retained personal information about the principal, but it does **not** include a prescriptive list of the information a business operator must disclose as part of a disclosure demand. However, the APPI states that the business operator 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 copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller

Business operators 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 business operator conducting its business, or violate other laws or regulations.

GDPR	APPI
Differences (cont'd)	
should be able to request, before the information is delivered, that the data subject specifies the information or processing activities to which the request relates.'	
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 business operator **must disclose personal data** pursuant to a cabinet order. A business operator should consider whether the procedures for receiving/responding to a request impose an excessive burden on a principal.
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 personal data is requested access to. In addition, Article 32(3) states that a request can be made through an agent pursuant to those prescribed by 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 business operators **may collect a fee** which is within a range recognised as reasonable considering the actual expenses when responding to a request.
Data subjects' requests must be complied with without '**undue delay** and in any event within **1 month** from the receipt of the request.' The deadline can be extended to **an additional 2 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 personal information handling business operator shall, when requested by a principal to be informed of a utilisation purpose of retained personal data that can identify them, inform the principal **without delay**, pursuant to a method prescribed by cabinet order.

4.5. 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 that withdrawal of consent must be without detriment.

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

4.6. Right to data portability

The GDPR has introduced the right to data portability, which is the right of individuals to obtain their personal data in a structured, commonly usable and machine-readable format when the processing is based on automated means and established through consent or contract. This right does not appear in the APPI.

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.

⚠ 5. Enforcement

5.1. Monetary penalties

Both the GDPR and the APPI provide for monetary penalties to be issued in case of non-compliance. However, only administrative penalties are stipulated in the GDPR, while criminal and non-criminal penalties are possible under the APPI. The laws also differ in how these penalties are enforced.

GDPR Article 83-84 Recitals 148-152	APPI 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, the **criminal penalty** may be up to:

- **JPY 1 million** (approx. €8,300) or imprisonment with work for not more than two years for a person that has used information 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. €4,150) or imprisonment with work for not more than one year for an operator, or its employees or former employees, that have handled private information 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. €2,500) 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)(3).

GDPR	APPI

Differences (cont'd)

- **JPY 300,000** for a person who has failed to submit a report or material under Article 40(1); falsely responded to, or refused, obstructed or evaded an inspection; or failed to submit a report or falsely submit a report under Article 56.
- **Non-criminal fines** of up to JPY 100,000 (approx. €830) 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

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 PPC as regulated by the APPI, does not have the power to issue monetary penalties.

Additionally, 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.

GDPR	APPI
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 to disclosure, correction, and utilisation cessation, 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.