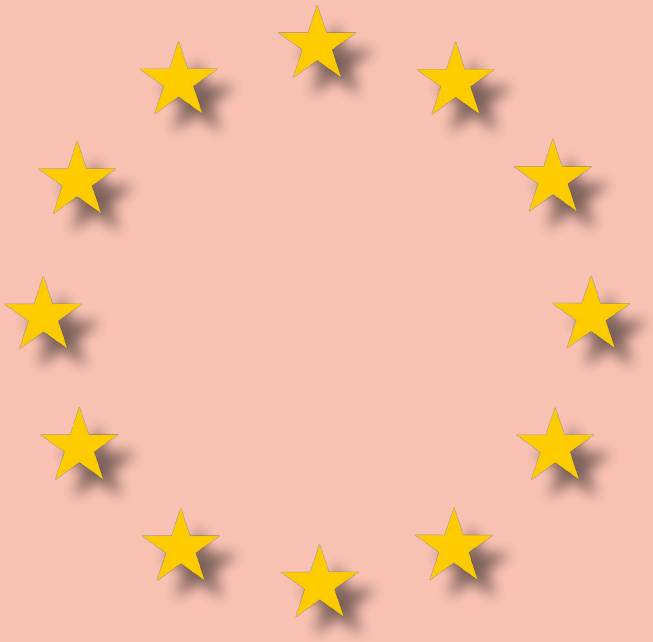
LATEST EDITION

Comparing privacy laws:
GDPR v. PIPA



May 2023

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

Lee & Ko 법무법인(유) 광장

About the authors

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

OneTrust DataGuidance™ Regulatory Research includes focused guidance around core topics (i.e. GDPR, data transfers, breach notification, among others), Comparisons 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 program.

Lee & Ko was founded in 1977 and consistently ranks among the largest and most highly respected law firms in Korea. With more than 700 professionals, organized into 40 practice groups, Lee & Ko is a premier full-service law firm whose clients benefit from the firm's unequalled depth of resources in terms of experience, professionalism and capabilities sufficient to expertly provide any legal services that may be required. As recognized by Korea's major media outlets and international law firm rating services, Lee & Ko enjoys one of the highest levels of client satisfaction and a particularly excellent reputation for the quality of the firm's legal services. Over the past 10 years, Lee & Ko has consistently been ranked as a top-tier law firm in various practice areas by Chambers Asia, Legal 500, Asia Law Profile and other reputable publications.

Contributors:
OneTrust DataGuidance™: Angela Potter, Keshawana Campbell, Bahar Toto, Victoria Ashcroft

Lee & Ko
Kwang Bae Park and Minchae Kang

Image production credits:
Cover/p.5/p.51: flowgraph / Essentials collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com
Icon p.33-40: AlexeyBlogoodf / Essentials collection / istockphoto.com
Icon p.47-51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com

Table of contents

Introduction

The Law on Personal Information Protection Act ('PIPA') came into force on 23 March 2011. Over the past decade, there have been several amendments to PIPA as well as enforcement decrees detailing associated requirements. PIPA provides personal data protection alongside two other notable pieces of legislation: the Use and Protection of Credit Information Act 2009 ('UPCIA') and the Act on Promotion of Information and Communications Network Utilization and Information Protection 2001 ('ICNA'). However, following major amendments that came into force on 5 August 2020, the role of the UPCIA and the ICNA in regard to personal data protection has significantly diminished through the transfer of their major relevant articles into PIPA.

These changes were part of South Korea's strategy to better align with the personal data protection obligations in the European Union and, as a result, receive an adequacy decision from the European Commission. For this reason, PIPA and the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') are fairly consistent in many aspects, although there remain several key distinctions.

For instance, while both pieces of legislation provide a broad scope within their jurisdictions, PIPA does not explicitly specify any potential extraterritorial scope. There are also inconsistencies between some key definitions, requirements, and legal bases for processing, such as the lack of definition for consent in PIPA and further processing without consent in research being prohibited under PIPA.

More significant differences between the legislations can be found in the requirements for data processing records and Data Protection Impact Assessments ('DPIAs'), whereby record keeping is not required under PIPA and DPIAs are only required for public authorities.

Both the GDPR and PIPA provide for the imposition of monetary penalties for non-compliance, with penalties potentially being calculated as a percentage of revenue. However, unlike the GDPR, PIPA provides for criminal sanctions, including imprisonment. In general terms, however, the GDPR and PIPA are comparable in their efforts to provide comprehensive protection for personal data, and both can be considered to be at the foundation of robust privacy frameworks. This guide is aimed at highlighting the similarities and differences between the PIPA, its Enforcement Decree of the Personal Information Protection Act ('Enforcement Decree'), and the GDPR in order to assist organisations in complying with both.

Structure and overview of the Guide

This Guide provides a comparison of the two legislative frameworks on the following key provisions:

1. Scope
2. Key definitions
3. Legal basis
4. Controller and processor obligations
5. Individuals' rights
6. Enforcement

Each topic includes relevant provisions from the two legislative frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and PIPA.

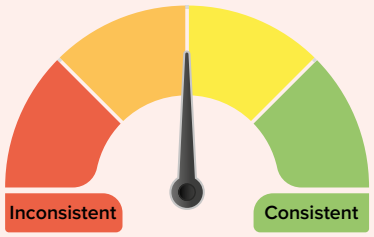
Key for giving the consistency rate

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

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

Inconsistent: The GDPR and PIPA 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 informational 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

Fairly consistent

Both the GDPR and PIPA protect living individuals with regard to the use of their personal data, utilise concepts that bear some degree of similarity, and both apply to private and public bodies.

GDPR Articles 3, 4(1) Recitals 2, 14, 22-25	PIPA Articles 2, 26

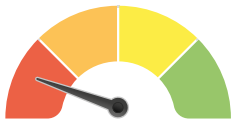
Similarities

The GDPR **only** protects **living individuals**. The GDPR does not protect the personal data of deceased individuals, this being left to Member States to regulate.	PIPA applies to the processing of personal information relating to **living natural persons only**. Data relating to the deceased is not included under the personal information protected by PIPA.
The GDPR defines a '**data controller**' as a 'natural and legal person, public authority, agency or other body which, alone or jointly, with others, determines the purposes and means of the processing of personal data.'	PIPA imposes specific obligations on '**data handlers**' which is a similar concept to that of a 'data controllers' under the GDPR. Under PIPA, a 'data handler' refers to 'a person (whether a public agency, juridical person, organisation, or individual) that, directly, or through a third party, handles personal information to make use of and/or carry out any operation of personal data files in the course of its work or in relation to its business/work/tasks.'
The GDPR defines a '**data processor**' as a 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'	Whilst PIPA does not utilise the concept of a 'data processor,' the term is similar to the concept of an '**outsourced processor**' or an 'outsourcee.' The 'outsourced processor' is defined in PIPA as 'a person (whether a public agency, juridical person, organisation, or individual) who undertakes processing of personal information outsourced by the data handler.'
Article 4(1) of the GDPR clarifies that a '**data subject**' is 'an identified or identifiable natural person.'	Under PIPA, '**data subject**' means 'an individual who is a subject of the handled data by which that individual can be identifiable.'
The GDPR **applies** to data controllers and data processors who may be **public bodies**.	PIPA **applies** to data handlers and outsourced processors who may be **public bodies**.

Differences

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.'	PIPA makes **no explicit reference** to its scope of application in relation to the nationality or place of residence of individuals.

1.2. Territorial scope



With regard to extraterritorial scope, the GDPR applies to data controllers and data processors that do not have a presence in the EU but have processing activities that take place in the EU.

While it is understood that PIPA applies to all data handlers and outsourced processors within South Korea, PIPA does not specify the territorial scope of PIPA. Furthermore, PIPA does not reference its extraterritorial scope, however in practice several factors are considered when deciding whether a foreign entity is subject to PIPA.

GDPR	PIPA
Articles 3, 4, 11 Recitals 2, 14, 22-25	Not applicable

Similarities

GDPR	PIPA
Not applicable.	Not applicable.

Differences

GDPR	PIPA
The GDPR **applies** to organisations that have presence in the EU. In particular under Article 3, the GDPR applies to entities or organisations established in the EU, notably 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.	PIPA **does not** specify its territorial scope. However, it is understood that PIPA applies to data handlers (whether a public agency, juridical person, organisation, or individual) in South Korea.
In relation to **extraterritorial scope**, the GDPR applies to the processing activities of data controllers and data processors that **do not have any presence in the EU**, where processing activities are related to the **offering of goods, or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU**.	PIPA makes **no explicit reference** to its extraterritorial scope. In general, however, several factors are considered in determining whether a foreign entity is subject to PIPA (e.g. whether the company provides services targeted at Koreans, whether the company generates revenue from doing business in South Korea).

1.3. Material scope

Fairly inconsistent

Both the GDPR and PIPA generally define personal data as information that directly or indirectly relates to an individual. Similarly, both laws provide exceptions for personal data processing that is for legal purposes, personal use, or certain media related purposes. Moreover, both define special categories of personal data.

However, the GDPR and PIPA vary regarding other aspects of material scope. For instance, the GDPR allows more exceptions for personal data processing, including academic or artistic purposes. In addition, unlike the GDPR, PIPA does not differentiate between automated and non-automated means of data processing.

GDPR	PIPA
Articles 2-4, 9, 26 Recitals 15-21, 26	Articles 2, 23, 24, 58, 58-2 Articles 18, 19 of the Enforcement Decree

Similarities

The GDPR defines '**personal data**' as 'any information' that directly or indirectly relates to an identified or identifiable individual. The GDPR does not apply to the personal data of deceased persons.

PIPA defines '**personal information**' as any data relating to a living natural person that (i) identifies a particular individual by their full name, resident registration number, image, or the like, (ii) even if it by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual (in such cases, whether or not the information may be 'easily combined' shall be determined by reasonably considering the time, cost, and technology used to identify the individual such as the likelihood that the other information can be procured), or (iii) is information under items (i) or (ii) above which is pseudonymised and thereby becomes incapable of identifying a particular individual without the use or combination of additional information for restoration to its original state.

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.'

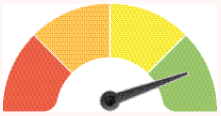
PIPA applies to the '**handling**' or '**processing**' of personal information which means 'collection, generation, recording, storage, retention, processing, editing, search, outputting, rectification, restoration, use, provision, disclosure, or destruction of personal information or any other action similar to any of the foregoing.'

The GDPR defines **special categories of personal data** as personal data revealing **racial or ethnic origin, political opinions, religious or philosophical beliefs, or 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**

PIPA defines '**sensitive (personal) information**' as '**personal information regarding an individual's ideology, faith, trade union or political party membership, political views, health, sexual orientation and other personal information that may cause a material breach of privacy**,' and further includes genetic information,

GDPR	PIPA
Similarities (cont'd)	
a natural person's sex life or sexual orientation. The GDPR also provides specific requirements for its processing.	criminal records, information on an individual's physical, physiological, and behavioural characteristics generated through certain technical means for the purpose of identifying a specific individual and racial/ethnic data. The Enforcement Decree defines 'unique identification data' ('UID') as the following: resident registration numbers ('RRNs'), driver's license numbers, passport numbers, and alien registration numbers. PIPA also provides specific requirements for the processing.of sensitive personal information and UID.
The GDPR excludes **anonymous data** from its application, which is defined as 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.	PIPA **does not** define anonymised data. However, PIPA expressly states that PIPA does not apply to the information by which the individual cannot be identified anymore when reasonably considering time, cost, technology etc.
The GDPR **excludes** from its application data processing in the context of **national security**.	Some of the PIPA provisions **do not apply** to the personal information which is collected and provided for the purpose of analysing information relating to **national security**.
Differences	
The GDPR **excludes** from its application the processing of personal data by individuals for **purely personal or household purposes**. This is data processing that has 'no connection to a professional or commercial activity.'	PIPA **does not** explicitly exclude the processing of personal data by individuals for personal or household purposes. However, PIPA's provisions regulating the collection of personal information, the requirements of a privacy policy, and the designation of a Privacy Officer do not apply when the data handler processes the personal information to manage organisations for personal friendship such as school reunions, or private clubs.
The GDPR **excludes** from its application data processing in the context of **law enforcement**.	PIPA **does not** explicitly exclude from its application data processing in the context of law enforcement.
The GDPR provides requirements for specific processing situations including processing for **journalistic purposes and academic, artistic or literary expression**.	PIPA **does not** provide requirements for specific processing situations including processing for academic, artistic, or literary expression. However, PIPA does exclude from its application personal information which is collected and used for the original purpose of the press, the religious organisations, the political party such as newsgathering, report, missionary work, recommendation of candidate etc.
The GDPR applies to the processing of personal data **by automated means or non-automated means if the data is part of a filing system**.	PIPA **does not differentiate automated and non-automated** means of processing of personal information.

2. Key definitions



Consistent

2.1. Personal data

Save for some difference in terminology, both the GDPR and PIPA share similar concepts of 'personal data' and 'personal information.'

GDPR	PIPA
Articles 4(1), 9 Recitals 26-30	Articles 2, 23, 24, 58-2 Articles 18 and 19 of the Enforcement Decree

Similarities

The GDPR defines '**personal data**' 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.'

PIPA defines '**personal information**' as any data relating to a living natural person, including: (i) information that identifies a particular individual by their full name, resident registration number, image, etc; (ii) information that, even if by itself does not identify a particular individual, may be easily combined with other information to identify a particular individual (in such cases, whether or not the information may be 'easily combined' shall be determined by reasonably considering the time, cost, technology, etc required to identify the individual, such as the likelihood that the other information can be procured); (iii) information that is under items (i) or (ii) which is pseudonymised and thereby becomes incapable of identifying a particular individual without the use or combination of additional information for restoration to its original state.

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.

PIPA defines '**sensitive information**' as personal information regarding an individual's ideology, faith, trade union or political party membership, political views, health, sexual orientation, and other personal information that may cause a material breach of privacy. In addition, the Enforcement Decree provides that the following also fall under the definition of sensitive information: genetic information, criminal records, information regarding an individual's physical, physiological, and behavioural characteristics generated through certain technical means for the purpose of identifying a specific individual and racial/ethnic data.

The GDPR applies to **pseudonymised information** to the extent that such data could still be attributed to a natural person by the use of additional information.

PIPA contains provisions applicable to **pseudonymised information**.

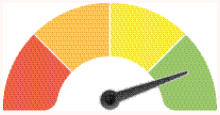
Similarities (cont'd)

The GDPR **does not** apply to 'anonymised' data, where the data can no longer be used to identify the data subject.	PIPA does not directly define anonymised data. However, PIPA expressly states that PIPA **does not apply to information by which the individual cannot be reasonably identified**, considering the time, cost, technology, etc. required to identify the individual, including the likelihood that other information can be procured.
The GDPR defines a '**filing system**' as any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.	PIPA defines a '**personal information file**' as a set or sets of personal information arranged or organised in a systematic manner based on a certain rule allowing for personal information to be searched easily.

Differences

The GDPR specifies that **online identifiers** may be considered as personal data, such as **IP addresses, cookie identifiers, and radio frequency identification tags**.	PIPA **does not** specify that online identifiers are considered as personal information. However, depending on the relevant circumstances, IP addresses, cookie identifiers, etc. may be viewed as personal information.
The GDPR **does not** directly refer to unique identifiers.	PIPA defines another special category of personal information, which is '**UID**.' The Enforcement Decree provides that UID includes resident registration numbers, driver's license numbers, passport numbers, and alien registration numbers.

2.2. Pseudonymisation



Consistent

Both the GDPR and PIPA provide a definition for pseudonymised data and state that such data is subject to the obligations of the GDPR and PIPA, respectively.

GDPR	PIPA
Articles 4(5), 11 Recitals 26, 29	Articles 2, 28-2

Similarities

The GDPR defines **pseudonymised data** as 'the processing of personal data in such a manner that the 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.'

PIPA defines **pseudonymised information** as data from which the specific individual cannot be identified without the use or combination of additional information for restoring to the original state.

Furthermore, PIPA defines 'pseudonymisation' as 'the processing of personal information to the extent where the specific individual cannot be identified anymore from that information without additional information, by deleting or replacing in whole or in part the personal information, or by any other means.'

Differences

Not applicable.

Not applicable.

2.3. Controllers and processors

Fairly consistent

Save for some differences in terminology, both the GDPR and PIPA share similar concepts of 'data controller' and 'data processor.' There are also common obligations under both laws, such as the requirement to appoint a data protection officer ('DPO') / privacy officer.

However, while the GDPR specifically provides that a data controller or data processor must conduct a Data Protection Impact Assessment ('DPIA') in certain circumstances, PIPA provides that only public organisations must conduct DPIAs in certain circumstances.

GDPR	PIPA
Articles 4, 17, 28, 30, 32, 33, 35, 37, 38 Recitals 64, 90, 93	Articles 2, 26, 31, 31-2, 33, 39-11 Articles 28, 48-9 of the Enforcement Decree

Similarities

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.	PIPA does not provide a definition of a data controller. Instead, PIPA defines a '**data handler**' as a public agency, legal person, organisation, or individual, that processes personal information, directly or indirectly, to operate personal information files as part of its activities. A 'personal information file' is defined as a set or sets of personal information arranged or systematically organised pursuant to certain rules for easy search or use of such personal data.
A **data processor** is a natural or legal person, public authority, agency or other body which processes personal data on **behalf** of the controller.	Whilst PIPA does not provide a definition of a data processor, the term is similar to the concept of an outsourced processor known as an '**outsourcee**.' An outsourcee may be a public agency, legal person, organisation, or individual that processes of personal information outsourced by the data handler.
The GDPR provides for the designation of a **data protection officer** ('DPO') by data controllers or data processors and defines the role of a DPO (see section 4.4.).	PIPA does not refer to the appointment of a DPO; instead PIPA provides for the designation of a **privacy officer** by data handlers and outsourced processors. In addition, data handlers that are also information and communications service providers ('ICSPs'), that do not have a place of business in South Korea, and meet certain standards set out in the Enforcement Decree of PIPA, must appoint a **domestic representative**. [This requirement previously applied only to information and communications service providers ('ICSPs') but will apply to all data handlers once the latest amendments to the PIPA go into effect on September 15, 2023. Unless specified otherwise in relation to the effective date, the same applies to the amended provisions in the amended PIPA.]

GDPR	PIPA

Similarities (cont'd)

The GDPR requires that processing by a processor is governed by **a contract or other legal act** under Union or Member State law.	PIPA requires data handlers to execute an **outsourcing contract** with the outsourcee that contains certain statutorily-prescribed matters, including but not limited to, prohibition on processing personal information for purposes outside the initial scope of the outsourcing, matters concerning liability, technical and managerial safeguards, as well as purpose and scope of the outsourcing.
The GDPR provides that where processing is to be carried out on behalf of a controller, the **controller shall use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.	PIPA requires data handlers to educate the outsourcee so that **personal data is not lost, stolen, leaked, forged, altered, or damaged** owing to the outsourcing of work, and to supervise how the outsourcee processes personal information safely by inspecting the status of processing.
The GDPR provides that the data processor shall not engage another data processor without prior specific or general written **authorisation** of the controller.	PIPA provides that the outsourcee shall not engage another sub-outsourcee without prior **authorisation** of the data handler.

Differences

The GDPR provides that a data controller or data processors conduct **DPIA** in certain circumstances (see section 4.3.).	PIPA **only requires public organisations** to conduct a DPIA.

2.4. Children

Fairly consistent

Both the GDPR and PIPA provides that the consent of a guardian or legal representative is required to process the personal information of children. However, PIPA does not contain provisions specifically targeted at protecting the personal information of children.

GDPR	PIPA
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	Articles 22-2, 38 Article 48-3 of the Enforcement Decree

Similarities

GDPR	PIPA
The GDPR **does not** define 'child' nor 'children.'	PIPA **does not** define 'child' nor 'children.'
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.	Data handlers that are information and communications service providers must communicate in an **easily understandable** form and use clear and plain language when notifying children of matters relating to the processing of personal information (applies only to ICSPs under the current PIPA)..
The GPDR provides that data controllers are required to make reasonable efforts to **verify** that **consent** is given or authorised by a parent or guardian.	PIPA does not contain general provisions as to the verification of consent. However, data handlers that are information and communications service providers are **required to confirm** whether the legal representative has granted consent (applies only to ICSPs under the current PIPA)..

Differences

GDPR	PIPA
Under the GDPR, 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**.	PIPA provides that when consent is required under PIPA to process the personal information of a child under the **age of 14**, the data handler must obtain the consent of the data subject's legal representative.
The GDPR **does not** contain an equivalent provision regarding the processing of personal information necessary to seek consent from the child's legal representative.	PIPA provides that when obtaining the consent of the child's legal representative, the data handler may, without the legal representative's consent, **collect information** directly from the child that is **necessary to seek consent** from the child's legal representative. In such case, the information to be collected directly from the child must be minimised to only what is necessary to seek consent of the legal representative and meet certain standards set out in the Enforcement Decree..
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.	PIPA **does not** contain provisions that provide specific protection when children's personal data is used for marketing or collected for information society services offered to a child.

2.5. Research

Fairly inconsistent

Unlike the GDPR, PIPA does not allow for the processing of personal data for research purposes without consent with limited exceptions.

However, both the GDPR and PIPA provide data subjects with the right to object to the processing of their personal data for research purposes, and provide a definition of scientific research.

GDPR	PIPA
Articles 5(1)(b), 9(2)(j), 14(5), 17(3), 21(6), 89 Recitals 33, 159-161	Articles 2, 15, 17, 37

Similarities

The GDPR clarifies that the processing of personal data for **scientific research** purposes should be interpreted 'in a broad manner including for example technological development and demonstration, fundamental research, applied research, and privately funded research.'

PIPA defines '**scientific research**' as 'research which applies scientific methods, such as development and demonstration of technology, fundamental research, applied research, research funded by private investment, etc.'

Under the GDPR, the data subject has the **right to object** to the processing of personal data for research purposes unless such research purposes are for reasons of **public interest**.

PIPA does not explicitly refer to the right to object in relation to data processing for research purposes, however a data subject is entitled to request the **suspension of the processing** of their personal information that is being processed by a data handler and the data handler must, without delay, suspend processing of some or all of the data subject's personal information, unless any of the following is applicable:

- where special provisions exist in law or it is inevitable to observe legal obligations;
- where it may possibly cause damage to the life or body of a third party, or improper violation of property and other interests of a third party;
- where the **public institution cannot perform its work** as prescribed by other laws without processing the personal information in question; or
- where the data subject fails to explicitly terminate a contract even though it is impracticable to perform the contract such as provision of service as agreed upon with the said data subject without processing the personal information in question.

GDPR	PIPA
Differences	
According to the GDPR, **the processing of sensitive data is not prohibited when 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'	Under PIPA, **sensitive information may only be processed with the consent** of the data subject or when specifically required or allowed under an applicable law. Accordingly, other than the fact that pseudonymised data may be processed without consent for purposes such as compiling statistics, conducting scientific research, and preserving records for public interest, the data subject's consent must be obtained in order to process personal information for research purposes.
The GDPR provides that 'further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), **not be considered to be incompatible with the initial purposes**'.	PIPA **does not** consider further processing specifically for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. However, personal information may be used or provided to a third party without the data subject's consent within the scope reasonably related to the original purpose of the collection after considering whether the contemplated use/provision is related to: • the original purpose of the collection; • whether such use/provision of the personal information could have been predicted in light of the circumstances surrounding the collection and customary handling practices; • whether the use/provision will not result in any disadvantage to the data subject; and/or • whether the data handler has implemented the necessary safeguards to ensure the security of the personal information (e.g. encryption). Whether research is a purpose for which further processing of personal information may occur without consent is assessed on a case-by-case basis and it is therefore difficult to draw a definitive conclusion.
Under the GDPR, where personal data are processed for research purposes, it is possible for **Member States to derogate from some data subjects' rights**, including the right to access, the right to rectification, the right to object and the right to restrict processing, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such **derogations** are necessary for the fulfilment of those purposes.	**Not applicable** to PIPA.

3. Legal basis

Fairly inconsistent

Unlike the GDPR, PIPA in principle requires explicit informed consent to be obtained for the processing of personal information after providing notice of certain matters prescribed by law, and separate consent must be obtained for each category of processing. Similarly to the GDPR, PIPA also recognises legitimate interest, performance of a contract, and other legal bases as valid grounds for processing personal information, however such legal bases are only recognised in limited scope.

GDPR	PIPA
Articles 4-10 Recitals 39-48	Articles 15, 16, 17, 22, 23, 24, 24-2 Article 17 of the Enforcement Decree

Similarities

The GDPR recognises **consent** as a legal basis to process personal data and includes specific information on how consent must be obtained and can be withdrawn.

PIPA recognises **consent** as the main legal basis to process personal information, and includes specific information on how consent must be obtained and can be withdrawn.

The GDPR states that data controllers can only process personal data when there is a legal ground for it. The legal grounds are:

- **consent**;
- when processing is necessary for 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;
- compliance with **legal obligations** to which the data controller is subject;
- to protect the **vital interest** of the data subject or of another natural person;
- performance carried out in the **public interest** or in the official authority vested in the data controller; or
- for the **legitimate interest** of the data controller when this does not override the fundamental rights of the data subject.

PIPA, in principle, requires explicit informed **consent** to be obtained for the collection and usage of personal information, unless one of the following exceptions apply:

- when required to comply with the data handler's **obligations under other applicable laws** or, it is specifically required or permissible under other applicable laws and regulations;
- when collection/use is necessary for a **public institution** to carry out its duties as prescribed by applicable laws and regulation;
- when collection or use is necessary to **perform a contract executed** with the data subject or implement measures in accordance with the request of the data subject during the process of entering into **a contract** (the requirements for the application of this exception have been relaxed vis-à-vis the current PIPA)
- where there is a **clear and urgent need to protect the life**, physical, or economic interest of the data subject or a third party;
- where required to achieve a **legitimate interest** of the data handler where the interest clearly overrides the rights of the data subject if the processing is substantially relevant to the legitimate interest of the data handler or a third party and the processing is within a reasonable scope; and
- when urgently necessary to ensure public safety and well-being, including public health

There are specific **legal grounds for processing special categories of data**, such as explicit **consent**.

Under PIPA, there are specific legal grounds for processing **sensitive personal information**, such as **consent**.

GDPR	PIPA

Similarities (cont'd)

	Nevertheless, resident registration numbers may not be processed even with the data subject's consent unless one of the following exceptions applies: • when it is required or permitted by certain laws or regulations; or • when it is clearly and urgently needed to protect the life, physical, or economic interest of the data subject or a third party.

Differences

The GDPR defines consent as 'any **freely given, specific, informed and unambiguous indication** of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.'	PIPA **does not define 'consent'**. However, PIPA stipulates that in order to obtain consent, the data handler shall present the request to the data subject in a clearly recognisable manner where each matter requiring consent is distinctly presented. Furthermore, the Supreme Court of Korea has issued rulings on how valid consent may be obtained.

4. Controller and processor obligations

4.1. Data transfers

Fairly inconsistent

Both the GDPR and PIPA regulate the transfer of data to third parties, including cross-border transfers. Similarly to the GDPR, the PIPA also recognises consent, international agreements, and other legal bases as valid grounds for cross-border transfers, and grants the PIPC to cease cross-border transfers in certain cases. With respect to the transfer of personal information to third parties, PIPA distinguishes between the 'provision' of personal information, which is similar to a data transfer between controllers under the GDPR, and the 'outsourcing' of the processing of personal information, which is similar to a data transfer between a controller and processor under the GDPR. Specifically, a provision of personal information refers to cases where a data transfer (that is beyond the original purposes for the collection/use of personal information) is conducted for the benefit and business purpose of the transferee, whereas outsourcing refers to cases where a data transfer (that is consistent with the original purposes for the collection/use of personal information) is conducted for the benefit and business purpose of the transferor.

GDPR	PIPA
Articles 44-50, 58 Recitals 101, 112	Articles 17, 26, 28-8, 28-9 Article 29 of the Enforcement Decree

Similarities

Under the GDPR, personal data may be transferred abroad with the **prior consent** of the data subject. Also, under the GDPR, a data transfer may take place when the it is necessary to protect the vital interests of a data subject or other persons.

Under the PIPA, with regards to the provision of personal data, the data handler must obtain the data subject's **explicit, prior consent** after notifying them of the statutorily-prescribed information regarding the provision. However, when it is clearly and urgently needed to protect the life, physical or economic interests of the data subject or a third party, provision may occur without the consent of the data subject. Also, the data handler is not required to obtain the data subject's consent for outsourced processing to third parties within Korea.

The GDPR provides for data transfers when the transfer is necessary for the performance or conclusion of a **contract**.

Under PIPA, with regards to outsourcing, the data handler must execute an **outsourcing contract** with the outsourcee that includes certain statutorily-prescribed information.

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.

Under the PIPA, personal information may be transferred to a third country or international organisation that is recognised by the Personal Information Protection Commission ('PIPC') as having **essentially equivalent levels of data protection as those required under the PIPA**.

The GDPR allows personal data to be transferred abroad when a data subject has explicitly **consented** to the proposed transfer and acknowledged the possible risks of such transfer due to inadequate safeguards.

Under the PIPA, personal information may be transferred cross-border when the data subject has separately given **consent**.

GDPR	PIPA

Similarities (cont'd)

GDPR	PIPA
The GDPR specifies that a cross-border transfer is allowed based on **international agreements** for judicial cooperation.	The PIPA allows a cross-border transfer when there are special provisions regarding the cross-border transfer in laws, **treaties or international agreements**.
Under the GDPR, cross-border transfers can be suspended pursuant to the corrective order of supervisory authorities.	Under the PIPA, cross-border transfers can be ceased pursuant to the order of the PIPC.

Differences

GDPR	PIPA
Under the GDPR, the following **legal grounds** can be applied to the transfer of personal data abroad: • 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.	PIPA **does not** include similar legal grounds for the provision of personal data abroad.
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 mechanism**.	Under PIPA, personal information may be transferred cross-border if the overseas transferee has obtained **data protection certification prescribed by the PIPC** and has taken all of the following measures: security measures necessary for the protection of personal information and **measures** necessary to guarantee the rights of the data subject; and measures necessary to conduct data processing in accordance with data protection certification in the country where personal information is to be transferred.
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.	Under the PIPA, the legal grounds for the cross-border transfer of personal information is allowed when (i) the outsourcing of the processing of personal information or the storage thereof is necessary for entering into or **performing a contract** and (ii) certain information that must be notified to the data subject when obtaining consent for the cross-border transfer has been disclosed in the **privacy policy** or notified individually to the data subject via methods prescribed by the Enforcement Decree (e.g., by email).

4.2. Data processing records

Fairly inconsistent

Neither the GDPR nor PIPA provide a general requirement for registering with supervisory authorities.

However, the GDPR requires data controllers and processors to maintain a record of processing activities, whereas PIPA does not impose specific record-keeping obligations for organisations' processing activities.

GDPR	PIPA
Article 30 Recital 82	Article 29, 30 Articles 30, 31 of the Enforcement Decree Articles 2, 8 of the Personal Information Safeguard and Security Standard

Similarities

The GDPR **does not** provide general requirements for registering with a supervisory authority.

The PIPA **does not** provide general requirements for registering with a supervisory authority.

Differences

Data controllers and data processors have an obligation to **maintain a record** of processing activities under their responsibility. The processing on information recorded by a data controller shall be in **writing or electronic form**. 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 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.

PIPA **does not** require organisations to maintain a record of processing activities. However, PIPA does require data handlers to manage and store log-in records which document the access to a data processing system by 'personal information handlers' (i.e. officers, employees, workers, etc. who process personal information under the direction and supervision of the data handler) for at least one year. Such log-in records shall contain the facts of access, including ID, date and time of access, information to identify the person of access, and tasks performed by the personal information handler while connected to the processing system.

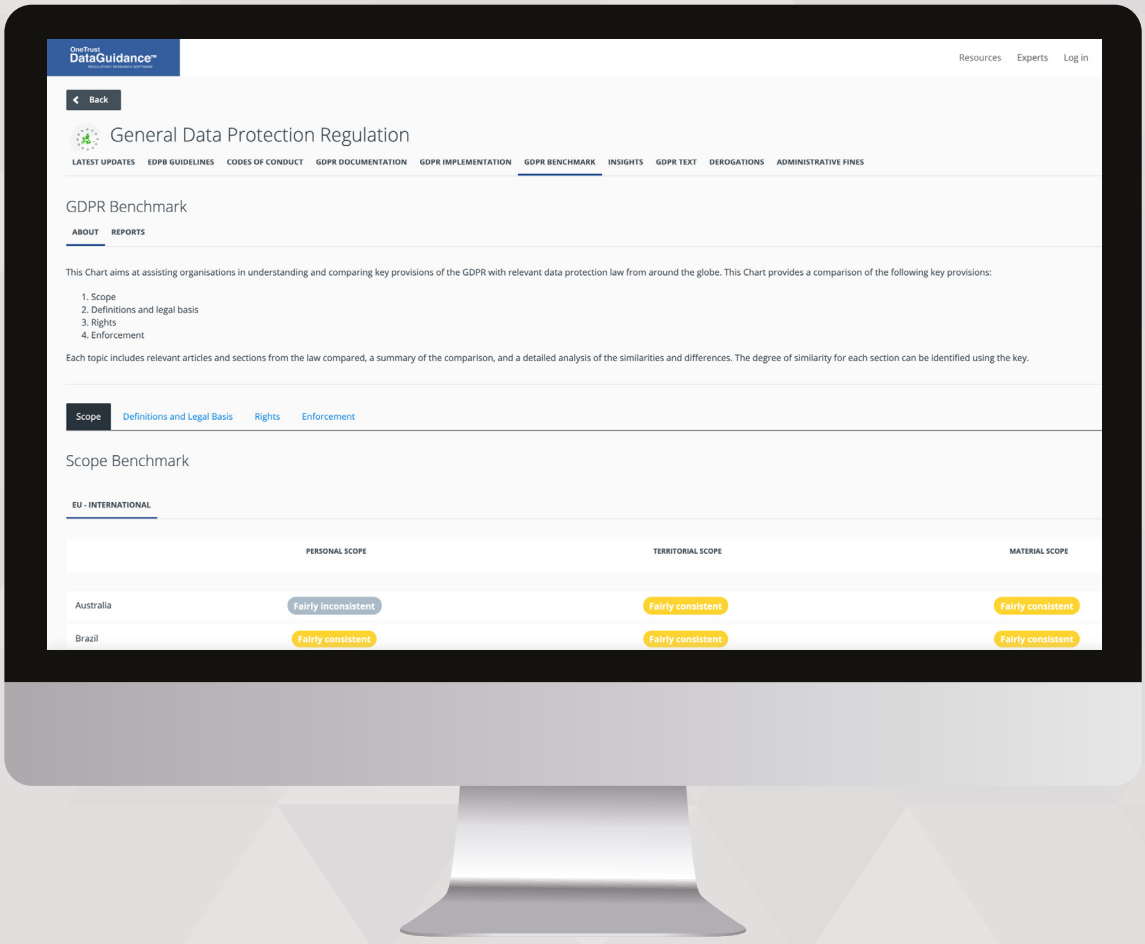
PIPA **does not** contain a list of information that a data handler must record. However, in relation to privacy policies, PIPA requires data handlers to disclose the following statutorily-prescribed information in a privacy policy:

- the **purposes of collection and use** of personal information, and the items of personal information collected;
- the names of any **third-party recipients** (e.g. person or company) to whom personal information is provided, the purposes of use of the personal information by such third-party recipients, and the items of personal information that are provided;

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	PIPA

Differences (cont'd)

	• the **periods of retention/use** of the personal information and the procedures/methods for destruction of the personal information (and if any personal information is required to be preserved under other applicable laws or regulations, the legal grounds thereof, and the specific items of personal information to be preserved); • in the event the processing of personal information is **outsourced** to a third party, the specific tasks that are outsourced and the name(s) of the third party to whom such tasks are outsourced; • (if applicable) (i) the possibility of the sensitive information may be disclosed and (ii) the methods on how to choose not to disclose the sensitive information; • (if applicable) matters regarding the processing of pseudonymised information, etc.; • the rights of data subjects and their legal representatives and the methods for exercising such rights; • the matters concerning the installation and operation of devices that automatically collects personal information, such as internet access information files, and the denial thereof; • the name and contact information of the person responsible for the management of personal information or the department responsible for performing tasks related to the protection of personal information and for handling related complaints; and • matters related to the implementation of security measures for the protection of personal information.
The obligations in relation to data processing records are also imposed on the **representatives of data controllers**.	PIPA **does not** impose record-keeping obligations on the representatives of data handlers in relation to processing personal information.
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.	PIPA **does not** prescribe a list of information that an outsourced processor must record.

GDPR	PIPA

Differences (cont'd)

The GDPR **prescribes a list of information that a data controller** must record regarding **international transfers** of personal data, with the identification of third countries or international organisations, and the documentation of adopted suitable safeguards.	PIPA **does not** prescribe a list of information that a data handler must record regarding international transfers of personal information.
The GDPR **does not** provide record-keeping obligations specific to the processing of pseudonymised information.	PIPA requires data controllers who intend to process **pseudonymised information** to prepare and keep records, including the purpose of processing the pseudonymised information and any third parties to which such information is provided.

4.3. Data protection impact assessment

Inconsistent

Whilst the GDPR provides that a DPIA must be conducted under certain specified circumstances, and makes no distinction between private or public entities with respect to this obligation, PIPA only requires public institutions to conduct a Privacy Impact Assessment ('PIA').

GDPR	PIPA
Article 35, 36 Recitals 75, 84, 89-93	Article 33

Similarities

GDPR	PIPA
Not applicable.	Not applicable.

Differences

Under the GDPR, a **DPIA must be conducted** under specific circumstances. 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.

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 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.

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 PIPA, **only public institutions** are obligated to conduct a PIA.

4.4. Data protection officer appointment

PIPA requires data handlers to appoint a privacy officer whose responsibilities are slightly different from those required of a data protection officer ('DPO') under the GDPR.

GDPR	PIPA
Articles 13 - 14, 37-39 Recital 97	Articles 30, 31 Article 32 of the Enforcement Decree

Similarities

Under the GDPR, data controllers and data processors, including their representatives, are required to **appoint** a DPO in certain circumstances.

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
- to act as a contact point to 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.

Contact details of the DPO must be included in the privacy notice for data subjects, and they must be communicated to the supervisory authority.

Under PIPA, data handlers must **appoint** a privacy officer who will be responsible for overseeing all data processing-related matters.

The privacy officer shall perform a list of tasks including:

- to establish and execute a plan to protect personal information;
- to carry out **routine check-ups** and improve actual conditions and practices concerning the processing of personal information;
- to respond to complaints relating to the processing of personal information, and provide remedies for damages incurred by data subjects;
- to establish an internal control system to prevent leaks, misuse, and abuse of personal information;
- to **plan and implement education programmes** about the protection of personal information;
- to protect, manage, and supervise personal data files;
- to take corrective measures immediately upon discovering any violations of personal protection laws, and report such corrective measures to the head of the organisation;
- to establish, modify, and implement the privacy policy pursuant to Article 30 of the PIPA;
- to maintain materials related with personal information protection; and
- to destroy personal information whose purpose of processing is attain or retention period expires.

Contact details of the privacy officer must be included in the privacy policy of data handlers. However, PIPA does not address whether this information must be communicated to the supervisory authority.

GDPR	PIPA

Similarities (cont'd)

The GDPR provides that the DPO **should not be dismissed or penalised** by the controller or processor for performing his/her tasks.	PIPA provides that the privacy officer may not be put at a **disadvantage or receive unfavourable treatment** from the data handler without a justifiable reason, while carrying out their duties as a privacy officer.
The DPO can be a **staff member** of the data controller or data processor or can perform tasks based on a **service contract**.	The Enforcement Decrees provides that the privacy officer must be either (i) the **owner** of the company or its representative, or (ii) an **officer** of the company (if the company has no officers, then the head of its department in charge of handling data protection/privacy-related matters).
The GDPR recognises the **independence** of DPOs.	PIPA provides that data handlers must ensure the independence of privacy officers when they are carrying out tasks (scheduled to go into effect on 15 March 2024).

Differences

Data subjects **may contact** the DPO with regard to the processing of their personal data as well as the exercising of their rights.	PIPA **does not** explicitly state whether data subjects may contact the privacy officer in relation to the processing of their personal data or the exercising of their rights. However, the contact details of the privacy officer must be included in the data handler's privacy policy.
Under the GDPR, 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 in their 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.)	Under PIPA, **data handlers** excluding those who meet certain standards (e.g. number of employees, amount of revenue, etc.) set out in the Enforcement Decree are required to appoint a privacy officer. For the data handlers who meet the standards set out in the Enforcement Decree and do not appoint a privacy officer, the owner or representative of the business becomes the privacy officer. (scheduled to go into effect on 15 March 2024).
A group may appoint a **single DPO** who must be easily contactable by each establishment.	PIPA provides that each data handler must appoint their own privacy officer, therefore a group of data handlers **cannot** appoint a single privacy officer.

4.5. Data security and data breaches

Both the GDPR and PIPA require organisations to implement appropriate security measures with respect to personal information. In addition, the GDPR and PIPA provide lists of physical, organisational, and technological measures that organisations may utilise in the safeguarding of personal information. Furthermore, both the GDPR and PIPA contain mandatory data breach notification provisions, however, the details of the notification requirements, such as timeline, and content of the notice, differ. Unlike the GDPR, under PIPA, data handlers who are not ICSPs are only required to notify the relevant authority if a data breach affects over 1,000 data subjects (however, this part may change following the amendment of the Enforcement Decree).

GDPR	PIPA
Article 5, 24, 32-34 Recitals 74-77, 83-88	Articles 3, 29, 34 Articles 30, 39, 40 of the Enforcement Decree

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.

Under PIPA, the data handler must **safely manage** the personal information by considering the likelihood of the data subject's rights being infringed upon and the risk associated with such infringement, depending on how the personal information is processed and the **type of processing involved**.

The GDPR states that **data controllers and data processors are required to implement appropriate technical and organisational security measures** to ensure that the processing of personal data complies with the obligations of the GDPR.

PIPA requires the data handler to take certain **technical, managerial, and physical measures** that are necessary to ensure the secure processing of personal information such that the personal information is not lost, stolen, divulged, forged, altered, or damaged.

The GDPR provides a **list** of **technical and organisational measures**, where appropriate, that data controllers and data processors may implement, such as:

- the pseudonymisation and **encryption** of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore **availability and access** to personal data in a timely manner in the event of physical or technical incident; and
- a process for regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The Enforcement Decree provides a **list** of **measures** data handlers can take to ensure the safety of personal information, including:

- establishing and implementing an internal management plan for handling personal information;
- **measures to control access** to personal information;
- application of **encryption** technology to safely store and transmit personal information;
- **measures to keep access records** and prevent forgery and alteration in response to personal information infringement incidents;
- installation and update of security programs for personal information; and
- physical measures such as provision of storage facilities for safe storage of personal information or installation of locking devices.

GDPR	PIPA

Similarities (cont'd)

GDPR	PIPA
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.	PIPA **provides a list of information** that must be, at minimum, included in the notification of the breach. For example, a notification must include the particulars of the personal information that was leaked.
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.	PIPA provides that a data handler must notify data subjects **without delay** upon becoming aware of a breach of personal information. In practice, without delay is construed to mean within five days of becoming aware of the breach, unless there is a justifiable reason for the delay. However, if the data handler is an ICSP, the notice must be made within 24 hours, unless there is a justifiable reason for the delay. However, if there is a justifiable reason, such as a case where the contact information of the data subject is unknown, other measures may be taken in lieu of notification as specified by the Enforcement Decree.

Differences

GDPR	PIPA
Under the GDPR, 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. 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.	Under PIPA, if the personal information above the scale prescribed by the Enforcement Decree of **1,000 or more individuals** is leaked, a report must be made to the regulator in writing without delay. In practice, this is construed to mean within five days of becoming aware of the breach.
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 is proportionate effort.	PIPA **does not** explicitly outline any exemptions in relation to notifying data subjects of a data breach. However, if emergency measures (e.g. blocking of access channels, inspection/ remedy of external and internal system vulnerabilities in the network or firewall, deletion of leaked personal data, retention of external access records for use in the investigation) are required to prevent the further spread or additional leakage of personal information, the data handler may implement such measures first and notify the data subject without delay after such measures have been taken. In practice, without delay is construed to mean within five days.

4.6. Accountability

Unlike the GDPR, PIPA does not explicitly refer to the term accountability, however it does state that data handlers should observe and perform such duties and responsibilities as provided for in PIPA. In addition, both pieces of legislation contain provisions that can be taken to apply to accountability such as the requirement to designate a data protection officer ('DPO') /privacy officer and establishment of a privacy policy.

GDPR	PIPA
Articles 5, 24-25, 35, 37 Recital 39	Article 3, 30, 31

Similarities

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.

PIPA does not explicitly refer to the term 'accountability,' however it states that 'the data handler shall endeavour to obtain the trust of data subjects by **observing and performing such duties and responsibilities as provided for in PIPA** and other related statutes.' Furthermore, accountability can be taken to apply to other requirements, including the appointment of a privacy officer and establishment of a privacy policy.

Differences

Not applicable.

Not applicable.

5. Rights

5.1. Right to erasure

Like the GDPR, PIPA also recognises the right to erasure, however there are some differences. Under PIPA, data handlers must respond to requests within 10 days, whereas under the GDPR data controllers must respond without undue delay and within one month from receiving a request. In addition, the GDPR includes provisions on personal data that has been made public by the data controller, while PIPA does not.

GDPR	PIPA
Articles 12, 17 Recitals 59, 65-66	Article 36 Articles 43, 46 and 47 of the Enforcement Decree

Similarities

The right to erasure applies to specific grounds, such as where **consent of the data subject is withdrawn** and there is **no other legal ground** for processing, or the personal data is **no longer necessary** for the purpose of which it was collected.

PIPA provides data subjects that have accessed their personal information with a **right to request the erasure** of such information from the relevant data handler. Under PIPA, data handlers **must disclose** what rights the data subjects have (e.g. right to erasure) in their privacy policy.

Under the GDPR, data subjects **must be informed** that they have the right to request for their data to be deleted and are entitled to ask for their data to be erased.

PIPA provides that data handlers, where necessary, have the ability to request relevant evidence necessary to confirm the erasure of personal information. In addition, the Enforcement Decree provides that **the data handler must confirm that the request is actually made by the data subject** whose personal information is to be deleted, or their appropriate legal representative.

The GDPR provides that a data controller must have in place **mechanisms** to ensure that **the request is made by the data subject** whose personal data is to be deleted. A request can be made in **writing, orally, and through other means including electronic means** where appropriate.

PIPA does not specifically address how requests should be made. However, the Enforcement Decree provides that a request must be made in accordance with the procedure determined by the data handler. Such procedure should meet the following requirements: (i) the methods available to the data subject in making the request need to be data subject-friendly, such as in **writing, by telephone or electronic mail, or via the Internet**; (ii) data subjects must be able to request erasure of their own personal information at least through the same window or in the same manner that the data handler uses to collect such personal information, unless a justifiable reason exists, such as difficulty in continuously operating such window; and (iii) the manner and procedure for the manner and procedure for exercising the right to request erasure is to be posted on a website if the handler operates the website.

GDPR	PIPA
Differences	
Under the GDPR, the right to erasure can be exercised **free of charge**. There may be some instances, however, where a fee may be requested, notably when requests are unfounded, excessive, or have a repetitive character.	Under PIPA, the data handler **may charge a processing fee** and postage to the data subject requesting erasure.
Data subject requests under this right must be replied to without 'undue delay and in any event within **one month** from the receipt of request.' The deadline can be extended by **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 data handler must respond to the data subject who requests erasure **within 10 days** of receiving the request. The response should either be confirmation that the data subject's personal information has been deleted (if the request was granted), or the fact that the request has been denied and the reasons for such denial and method of objecting to such denial.
Exceptions to the right of erasure provided by the GDPR include: • **freedom of expression** and freedom of information; • complying with **public interest purposes in the area of public health**; • establishment, exercise, or defence of **legal claims**; and • **complying with legal obligations** for a public interest purpose.	PIPA provides that erasure is not permitted when the collection of the said personal information is required by **other laws**.
Under the GDPR, if the data controller has made personal data public and is obliged to erase the personal data, the data controller, taking into account the available technology and the cost of implementation, shall take reasonable steps, including **technical measures**, to **inform controllers** processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, such personal data.	PIPA **does not** include separate provisions on the erasure of public personal information.

5.2. Right to be informed

Fairly consistent

The GDPR and PIPA both require data controllers to inform data subjects about the purpose for which their personal data is collected and processed. However, unlike the GDPR which recognises the right to be informed as a separate right, PIPA imposes an obligation on data handlers to disclose information regarding the processing of personal information to data subjects when obtaining consent as well as in a privacy policy accessible to the public.

GDPR	PIPA
Articles 5-14, 47 Recitals 58-63	Articles 15, 17, 20, 30, 37-2 Article 31 of the Enforcement Decree

Similarities

Under the GDPR, data subjects have the right to receive information on the following at the time of collection:

- the **identity and the contact details of the controller** or controller's representative;
- the **contact details of the DPO**;
- the **purposes of the processing** as well as the **legal basis for the processing**;
- any **legitimate interests** pursued by the controller or by a third party, if applicable;
- the **recipients or categories of recipients** of the personal data, if any;
- where applicable, the fact that the controller intends to **transfer personal data to a third country** and related information;
- the **period for which the personal data will be stored**, or if that is not possible, the criteria used to determine that period;
- the **data subject's rights**;
- whether the provision of personal data is an **obligation**;
- the existence of **automated decision-making**, including profiling.

In addition, data subjects must be informed of the **possible consequences** of a failure to provide personal data whether in complying with statutory or contractual requirements, or a requirement necessary to enter into a contract.

Under PIPA, data handlers must inform a data subject of the following when they obtain consent from the data subject to collect their personal information:

- the **particulars** of the personal information to be collected;
- the purpose for the collection and use of personal information;
- the period for **retaining** and using personal information; and
- the fact that the data subject is entitled to **deny consent**, and disadvantages, if any, resulting from the denial of consent.

In addition, the data handler must include the following statutorily-prescribed information in its privacy policy to be disclosed to the data subjects:

- the **purposes of collection and use** of personal information, and items of personal information collected;
- the names of any third-party (e.g. person or company name) **recipients** to whom personal information is provided, purposes of use of the personal information by such third-party recipients, and the items of personal information that are provided;

GDPR	PIPA
Similarities (cont'd)	
	• the **periods of retention/use** of the personal information and the procedures/methods for destruction of the personal information (and if any personal information is required to be preserved under other applicable laws or regulations, the legal grounds thereof, and the specific items of personal information to be preserved); • in the event the processing of personal information is **outsourced** to a third party, the specific tasks that are outsourced and the name(s) of the third party to whom such tasks are outsourced; • (if applicable) (i) the possibility of the sensitive information may be disclosed and (ii) the methods on how to choose not to disclose the sensitive information; • (if applicable) matters related to the processing of pseudonymised information, etc.; • the rights of data subjects and their legal representatives and the methods for exercising such rights; • the matters concerning the installation and operation of devices that automatically collects personal information, such as internet access information files, and the denial thereof; • the name and contact information for the **person responsible for the management of personal information** or the department responsible for performing tasks related to the protection of personal information and for handling related complaints; and • matters related to the implementation of **security measures** for the protection of personal information.
Data subjects must be **informed** of the existence of automated decision-making, including profiling, at the time when personal data is obtained.	Under the PIPA, a data subject has the right to **request an explanation** from the data handler in case of automated decision-making (scheduled to go into effect on 15 March 2024).
Data subject shall have the **right not to be subject to a decision based solely on automated processing**, including profiling, **which produces legal effects** concerning them or similarly significantly affects them.	Under the PIPA, a data subject has the **right not be subject to automated decision-making** in certain cases when automated decision-making is likely to affect/has **affected their rights or obligations significantly**, except when such decision-making is made on the basis of data subjects' consent, legal provisions or the need for the execution/ performance of a contract between the data subjects and the data handler (scheduled to go into effect on 15 March 2024).

GDPR	PIPA
Differences	
Information should be provided to data subjects in an easily accessible form with clear and plain language, which can be in **writing and other means such as an electronic format**.	When obtaining consent from the data subject regarding the collection/use of personal information and the provision of personal information to a third party, the data handler must also notify the data subject of the fact that he/she is entitled to refuse consent and **any disadvantages** the data subject may face if he/she fails to provide consent. In principle, the privacy policy must be posted on the data handler's **website**. If this is not possible, the privacy policy must be published through certain methods, including but not limited to, posting it in an easily noticeable place at the data handler's place of business.
A data controller cannot collect and process personal data for purposes other than the ones about which the data subjects were informed, **unless the data controller provides them with further information**. Information relating to personal data processing (e.g. the purpose of the processing, the rights of data subjects, etc.) must be provided to data subjects by the data controller **at the time when personal data is obtained**.	Under PIPA, the data handler may not process personal information for purposes other than those to which the data subject has consented. However, such processing is possible **if consent is obtained regarding the additional purpose**. Personal information may also be processed without the data subject's additional consent if the purpose is reasonably related to the original purpose of collection, such determination to be made by considering whether the data subject would experience any disadvantage as a result of the processing, whether measures to secure safety, such as encryption, have been taken, etc. The collection/use of personal information as well as the provision of personal information to a third party **may occur only after** statutorily prescribed information (e.g. items of personal information to be processed, retention period) relating to personal information processing is notified to data subjects and their consent is obtained.
A data controller must **inform** data subjects of the existence or absence of an adequacy decision, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference the **appropriate or suitable safeguards** and the means by which to obtain a copy of them or where they have been made available.	PIPA **does not** contain a similar requirement.
The GDPR provides specific information that must be given to data subjects when their personal data has been **collected from a third party**, which includes the sources from which the data was collected.	PIPA provides specific information that must be provided immediately at the request of a data subject when their personal information has been collected from a third party, which includes the sources from which the data was collected.

GDPR	PIPA
Differences	
In the case of indirect collection, a data controller must provide information relating to such collection to data subjects 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 is first disclosed to the recipient**.	However, data handlers who meet certain criteria must provide such information within **three months** of receiving the data from a third-party source, even if there is no request from the data subject.
Information can be provided to data subjects **orally**, in addition to in writing form or electronic means.	The privacy policy containing information about data processing must be provided to data subjects in **writing**.
The GDPR provides examples of circumstances, which can be considered as '**legitimate interest**.'	The PIPA recognises 'legitimate interest' grounds, but only in very **limited** instances.

Fairly consistent

5.3. Right to object

Both the GDPR and PIPA recognise the right to restrict processing and require that data subjects be informed of this right, although the rights contain notable differences.

GDPR Articles 7, 12, 18, 21	PIPA Articles 37, 39-7 Articles 44 and 47 of the Enforcement Decree

Similarities

Data subjects shall have the right to **withdraw** their consent to the processing of their personal data at any time.	Data handlers must allow data subjects to **withdraw** their consent to the processing (e.g., collection/ use, Provision) of their personal information unless one of the following exceptions applies: where special provisions exist in law or it is inevitable to observe the data handler's legal obligations; where access may possibly cause damage to the life or body of a third party, or unfairly infringe upon a third party's property or other interest; or where the data handler would not be able to perform the terms of a contract executed with the data subject if it does not process the personal information and the data subject did not clearly indicate their intention to terminate the contract (applies only to ICSPs under the current PIPA).
The GDPR establishes a **right to restrict processing** where: • the accuracy of the personal data is contested by the data subject; • the processing is unlawful and the data subject opposes the erasure of the personal data; • the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject; • pending the verification of whether the legitimate grounds of the controller override those of the data subject.	Data handlers must respond to a data subject's r**equest to suspend** the processing of their personal information. Data handlers must comply with a data subject's request to suspend processing of their personal information unless one of the abovementioned exceptions applies.
The data subject has the right to be **informed** about the right to object.	Data handlers must disclose what rights the data subjects have (e.g. right to request suspension of processing and right to withdraw consent) in their privacy policy.
Data subjects must be **provided with information** about **how to exercise** the right.	The request must be made in accordance with the procedure determined by the data handler. Such procedure should meet the following requirements:

GDPR	PIPA

Similarities (cont'd)

	(i) the methods available to the data subject in making the request need to be data subject-friendly, such as in writing, by telephone or electronic mail, or via the Internet; (ii) data subjects must be able to request suspension of their own personal information or withdrawal of consent at least through the same window or in the same manner that the data handler uses to collect such personal information, unless a justifiable reason exists (e.g. difficulty in continuously operating such window), and (iii) details regarding the manner and procedure for exercising the right to request suspension/withdrawal or consent is to be posted on the website operated by the data handler (if such website exists).

Differences

Under the GDPR, data subjects are provided with the right to object to the processing of their personal data in specific circumstances: • the processing of personal data is due to **tasks carried out in the public interest** or **based on a legitimate interest pursued by the data controller** or **third party**; • the processing of personal data is for **direct marketing purposes**; and • the processing of personal data is for **scientific, historical research or statistical purposes**. Upon the receipt of an objection request, a data controller shall no longer process the personal data unless: • **the processing is based on a legitimate ground** that overrides the data subjects' interests; or • **it is for the establishment, exercise, or defence of a legal claim**.	PIPA **does not** contain similar provisions regarding the right to object.

5.4. Right of access

Fairly consistent

Both pieces of legislation guarantee a data subject's right to access. However, the GDPR and PIPA contain minor differences including the amount of information that should be included in a response, the restrictions on the exercise of this right, and timelines.

GDPR	PIPA
Articles 15 Recitals 59-64	Article 35 Articles 41, 42, 46, and 47 of the Enforcement Decree

Similarities

The GDPR recognises that data subjects have the **right to access** their personal data that is processed by a data controller.

Under PIPA, a data subject may **request access** to their personal information processed by the data handler.

The GDPR provides that the right of access **must not adversely affect the rights or freedoms of others**.

PIPA establishes that the right of access may only be **limited or denied** in circumstances where: (i) such access is prohibited or restricted by law; or (ii) it may possibly cause **damage to the life or body of a third party, or improperly violate the property and other interests of a third party**.

The GDPR specifies that, **when responding to an access request**, the data controller must indicate the following information:

- the **purposes** of the processing;
- the **categories** of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been or will be **disclosed**, in particular recipients in third countries or international organisations;
- where possible, the envisaged **period** for which the personal data will be **stored**, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller **rectification or erasure** of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a **complaint** with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their **source**; and
- the existence of **automated decision-making**, including profiling.

The Enforcement Decree specifies that the data subject may request access to any of the following information from the data handler:

- the **items** of personal information concerned;
- the purpose for collecting/using the personal information;
- the **retention and use period** of the personal information;
- the status of any **provision** of personal information to third parties; and
- the fact that the data subject consented to the data handler's processing of personal information.

Data subjects must have a variety of means through which they

PIPA provides that a request must be made in accordance

GDPR	PIPA

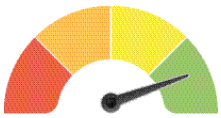
Similarities (cont'd)

can make their request, including **orally and through electronic means**. In addition, when a request is made through electronic means, a data controller should submit a response through the same means.	with the procedures determined by the data handler. Such procedure should meet the following requirements: • the methods available to the data subject in making the request need to be data subject-friendly, such as in **writing, by telephone, or electronic mail**, or via the internet; • data subjects must be able to request access at least through the same window or in the same manner that the data handler uses to collect such personal information, unless a justifiable reason exists (e.g. difficulty in continuously operating such window); and • details regarding the manner and procedure for exercising the right to request access is to be posted on the website operated by the data handler (if such website exists).
The GDPR specifies that a data controller must **have in place mechanisms** for **identity verification**.	PIPA establishes that data handlers must **confirm that the request is made by the data subject** whose personal information is to be accessed, or their appropriate legal representative.

Differences

A data controller can refuse to act on a request when it is **manifestly unfounded, excessive, or has a repetitive character**.	This PIPA **does not** contain an equivalent provision.
Data subjects' requests under this right must be replied to without 'undue delay and in any event within **one month** from the receipt of a request.' The deadline can be extended by **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such an extension within one month from the receipt of a request.	The data handler must respond to the data subject who requests access within **10 days** of receiving the request. The response should either be the granting of access (if the request was accepted), or the fact that access has been put on hold, in which case the grounds for the delay must be explained. Once the reason for delay no longer exists or is cured, access must be granted without delay.
The right to access 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 data handler may charge a **processing fee and postage** to the data subject requesting access.

5.5. Right not to be subject to discrimination



Consistent

The right not to be subject to discrimination in exercising rights is not explicitly mentioned in the GDPR or PIPA. However, under the GDPR and PIPA the right not to be subject to discrimination can be implied from the fundamental rights of the data subject.

GDPR	PIPA
Not applicable	Not applicable

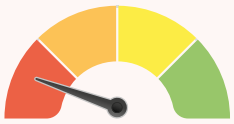
Similarities

GDPR	PIPA
The GDPR **does not** explicitly address the right not to be subject to discrimination; therefore, no scope of implementation is defined.	The PIPA also **does not** explicitly address the right not to be subject to discrimination.

Differences

GDPR	PIPA
Not applicable.	Not applicable.

5.6. Right to data portability



Both the GDPR and the PIPA recognise the right to data portability, however, the two laws define the right to data portability differently. The effective date of the relevant provisions in the amended PIPA relating to the right to data portability has not yet been determined but is expected to be sometime after 15 March 2024.

GDPR	PIPA
Articles 12, 20, 28 Recitals 68, 73	Article 35-2, 35-3

Similarities

The GDPR defines the right to data portability as the **right to receive data processed on the basis of contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format'** and to transmit that data to another controller without hindrance.

Under the PIPA the right to portability refers to the **right to request to the data handler which meets certain standards set out in the Enforcement Decree for transmission of personal information to either the data subject themselves or a third party**, so long as such personal information is **not generated from analysis/processing of the same collected by the data handler** and meets the following criteria: the personal information must have been (i) processed based on the consent of the data subject; (ii) processed to perform a contract executed with the data subject or to implement measures requested by the data subject in course of executing the contract; or (iii) **designated by the PIPC** pursuant to a request from a central administrative agency for the data subject's or public interest in cases where the transmission thereof is permitted by or unavoidably necessary for compliance with law; is unavoidably necessary for a public institution to conduct its statutorily prescribed tasks; or concerns sensitive information or UID and its processing is permitted or required by law; and the personal information must have been **processed by an information processing device such as a computer**. Upon request from the data subject, the data handler must transmit the personal information in a format that can be processed through a data processing device such as a computer, to the extent technically feasible and reasonable in terms of time and cost.

The GDPR provides that the right to portability must not adversely affect the rights and freedoms of others.

The PIPA provides that the right to portability must not infringe on the rights or legitimate interests of others.

GDPR	PIPA

Differences

The GDPR **does not** contain an equivalent provision.	Under the PIPA, in case of requests for transmission to a **third party**, the third party must be a professional institution specialized in personal information management ('Specialised Institution') or another **data handler that has implemented the requisite technical, managerial, and physical security measures and has satisfied relevant standards for facilities/equipment** prescribed by the PIPA and the Enforcement Decree. The Specialised Institution must be designated by the PIPC or relevant central administrative agency (the provision on 'Specialised Institution' is scheduled to go into effect on 15 March 2024).

6. Enforcement

Fairly inconsistent

6.1. Monetary penalties

Both the GDPR and PIPA provide for the imposition of monetary penalties for non-compliance. However, unlike the GDPR, PIPA provides for criminal sanctions, including imprisonment.

GDPR	PIPA
Article 83, 84 Recitals 148-149	Articles 64-2, 70, 71, 72, 73, 74, 75

Similarities

Under the GDPR, fines may be **issued directly** by the supervisory authorities.

Under PIPA, fines may be **issued directly** by the PIPC.

When applying an administrative sanction, the supervisory authority must consider:

- the nature, gravity and duration of the infringement;
- the intentional or negligent character of the infringement;
- any action taken to mitigate the damage;
- the degree of responsibility of the controller or processor;
- any relevant previous infringements;
- the degree of cooperation with the supervisory authority;
- the categories of personal data affected by the infringement;
- the manner in which the infringement became known to the supervisory authority;
- where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
- adherence to approved codes of conduct or approved certification mechanisms; and
- any other aggravating or mitigating factor applicable to the circumstances of the case.

Depending on the violation occurred the penalty may be up to 3% of the total sales revenue unless the data handler can successfully argue for the exclusion of any sales revenue unrelated to the activity in violation of the PIPA. However, in cases where there is no revenue or it is difficult to calculate revenue, as determined by the Enforcement Decree, a penalty not exceeding KRW 2 billion (approx. €1,417,910) may be imposed. Further, if the data handler refuses to submit sales calculation data without a justifiable reason or submits any false data, the upper limit of the penalty may be calculated based on 3% of total sales revenue. The regulator may reduce the penalty surcharge amount so calculated by up to 90%, or allow exemption of the said amount, by taking into account the factors prescribed in the Enforcement Decree. The regulator may reduce or waive administrative fine considering severity, motivation, or results of the activity in violation of the PIPA, the scale of the data handler, etc. The criteria used for determining the specific amount of the administrative fine are set forth in the Enforcement Decree.

Depending on the violation 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. **When applying an administrative sanction, the supervisory authority must consider**: (i) the nature, gravity, and duration of the infringement; (ii) the intentional or negligent character of the

When imposing a penalty surcharge, the regulator must consider the following factors, the details of which are set forth in the Enforcement Decree: (i) the substance and severity of the violation; (ii) the period and frequency of the violation(s); (iii) the benefit gained as a result of the violation; (iv) the extent to which the data handler endeavoured to implement security measures such as encryption; (v) (in case of data breach) relevance to

GDPR	PIPA

Similarities (cont'd)

infringement; (ii) the intentional or negligent character of the infringement; (iii) any action taken to mitigate the damage; (iv) the degree of responsibility of the controller or processor; (v) any relevant previous infringements; (vi) the degree of cooperation with the supervisory authority; (vii) the categories of personal data affected by the infringement; (viii) the manner in which the infringement became known to the supervisory authority; (ix) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (x) adherence to approved codes of conduct or approved certification mechanisms; and (xi) any other aggravating or mitigating factor applicable to the circumstances of the case.	the violation and the extent to which the personal information in question was damaged, stolen, lost, leaked, fabricated; (vi) whether the data handler took any post- infringement action to mitigate the damage; (vii) the type of work performed by the data handler and the scale thereof; (viii) the type of personal information that the data handler processes and the impact on the data subject, (ix) the extent of damage to the data subject due to the violation, (x) efforts to protect personal information, such as personal information protection certification and voluntary data protection activities; and (xi) actions taken to rectify violations, such as cooperation with the PIPC.

Differences

Depending on the violation 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 PIPA provides for several levels of penalty surcharges and administrative fines, including: 3% of the total sales revenue unless the data handler can successfully argue for the exclusion of any sales revenue unrelated to the activity in violation of the PIPA. However, in cases where there is no revenue or it is difficult to calculate the revenue, as determined by the Enforcement Decree, a penalty not exceeding KRW 2 billion (approx. €1,417,910) may be imposed. and for other administrative offences, between KRW 10 million to KRW 50 million (approx. €7,090 to €35,450).
The GDPR provides for the possibility of administrative, **monetary penalties** to be issued by the supervisory authorities in cases of non-compliance.Under the GDPR, it is left to **Member States to create rules** on the application of administrative fines to public authorities and bodies.	PIPA provides the possibility of **administrative fines and penalty surcharges** to be issued by regulators, as well as criminal penalties (both imprisonment and criminal fines) to be imposed by the court, in cases of non-compliance.
The GDPR **does not** establish provisions for imprisonment.	PIPA establishes provisions for **imprisonment**.
The GDPR **does not** establish DPO or individual liabilities.	Imprisonment and criminal fines are penalties imposed on the **individual** associated with the violation.

6.2. Supervisory authority

Fairly consistent

Under the PIPA, the PIPC has been assigned to handle tasks related to the protection of personal data as is the case under the GDPR. In addition, both the GDPR and PIPA provide supervisory authorities with wide-ranging investigatory powers and corrective powers.

GDPR	PIPA
Articles 51-84 Recitals 117-140	Articles 7, 7-8, 28-9, 64, 64-2, and 75

Similarities

Under the GDPR, supervisory authorities have **investigatory powers** which include:
(i) ordering a controller and processor to provide information required;
(ii) conducting data protection audits;
(iii) carrying out a review of certifications issued; and
(iv) obtaining access to all personal data and to any premises.

Under PIPA, the PIPC is assigned with the role of supervisory authority and is responsible for carrying out the following tasks:
(i) improvement of laws and regulations related to the protection of personal data;
(ii) establishment and implementation of policies, programs, and plans related to the protection of personal data;
(iii) **investigation** of alleged infringement of the rights of data subjects and determination of administrative measures related thereto;
(iv) handling of **complaints** and provision of redress related to the processing of personal data and mediation of disputes related to personal data;
(v) international exchange and cooperation with international data protection organisations and foreign data protection authorities;
(vi) conducting surveys, research, training, and **promotion of laws/regulations**, policies, programs, and compliance related to the protection of personal data;
(vii) supporting the development/dissemination of technology, standardisation of technology, and **training of professionals** related to the protection of personal data; and
(viii) any other tasks assigned to the PIPC under PIPA and other laws/regulations.

Under the GDPR, supervisory authorities shall also handle **complaints** lodged by data subjects. Under the GDPR, supervisory authorities are tasked with **promoting public awareness** and understanding of the risks, rules, safeguards and rights in relation to processing as well as **promoting the awareness of controllers and processors** of their obligations, amongst other tasks.

Under PIPA, the PIPC may order anyone who has violated PIPA to take any of the following measures:
(i) **cease engagement of the personal data infringement activity**;
(ii) **temporarily suspend** the processing of personal data; and
(iii) any other measures necessary for the protection of personal data and the prevention of the infringement of personal data.

GDPR	PIPA

Similarities (cont'd)

Under the GDPR, supervisory authorities have **corrective powers** which include:
(i) issuing warnings and reprimands;
(ii) imposing a **temporary or definitive limitation** including a **ban on processing**;
(iii) ordering the rectification or erasure of personal data;
(iv) imposing **administrative fines**; and
(v) ordering the suspension of data flows to a recipient in a third country or to an international organisation.

In addition, the PIPC may impose **administrative fines** and **penalty surcharges** for violations of PIPA, and where criminal punishment is prescribed, refer such violations to the investigative authorities for criminal prosecution. Under the PIPA, the PIPC has the authority to order data handlers to cease cross-border transfers of personal information in certain cases.

Differences

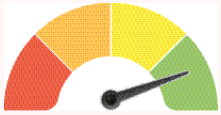
It is **left to each Member State to establish a supervisory authority**, and to determine the qualifications required to be a member, and the obligations related to the work, such as duration of term as well as conditions for reappointment.

Supervisory authorities may be subject to financial control only if it does not affect its **independence**. They have separate, public annual budgets, which may be part of the overall national budget.

Under PIPA, **the PIPC is the central administrative agency** established to independently conduct work related to the protection of personal information. PIPA outlines the composition of the PIPC, the term of office and grounds for disqualification.

Under PIPA, there is **no provision** which addresses matters related to the budget of the PIPC.

6.3. Other remedies



Consistent

PIPA is similar to the GDPR in that data subjects are entitled thereunder to, among other things, seek compensation for damages and participate in class action litigation.

GDPR Articles 79, 80, 82 Recitals 131, 146-147, 149	PIPA Article 39, 49, 51

Similarities

The GDPR provides individuals with a cause of action to **seek compensation** from a data controller and data processor for a violation of the GDPR.

Under PIPA, data subjects may **seek compensation** against data handlers for any damages they suffer due to violations committed by such data handlers. In such cases, data handlers will be held liable for the damages suffered by data subjects unless they can prove that they were neither intentionally nor negligently at fault for such damages.

The GDPR provides that a data controller or processor shall be exempt from liability to provide compensation if it proves that it is not in any way responsible for the event giving rise to the damage.

In addition, data handlers may be held liable under PIPA for up to five times (up to three times under the currect PIPA) the amount of damages suffered by data subjects in connection with any loss, theft, leakage, falsification, alteration, or damage of personal data caused by their intentional or grossly negligent acts or omissions. In such cases, data handlers may avoid liability if they can prove that they were neither intentionally nor grossly negligently at fault for the damages suffered by data subjects.

The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to **a not-for-profit body, association, or organisation** that has as its statutory objective the protection of data subject rights.

If multiple data subjects have suffered the same or similar types of damages or infringement of their rights due to a data handler's alleged actions/inactions of a similar nature, such data subjects may collectively request mediation against the data handler to resolve their disputes together.

If the data handler rejects the collective mediation request, the data subjects would be entitled to initiate class action litigation directly against the data handler through a **consumer organisation** under the Framework Act on Consumers 2006 (as amended) or a **non-profit organisation** under the Assistance for Non-Profit and Non-Governmental Organizations Act 2017.

Under the GDPR, the data subject has the right to **lodge a complaint** with the supervisory authority. The supervisory authority must inform the data subject of the progress and outcome of their complaint.

PIPA does not explicitly provide data subjects with the right to lodge a complaint with the supervisory authority. However, it is generally understood that **data subjects may lodge such complaints** with the supervisory authority as the

GDPR	PIPA
Similarities (cont'd)	
	handling of complaints related to the processing of personal information is one of the tasks enumerated in PIPA that the PIPC is required to carry out.
Differences	
Not applicable.	Not applicable.

PROVIDING SOLUTIONS, NOT JUST ANSWERS.

Lee & Ko 법무법인(유) 광장

63, Namdaemun-ro, Jung-gu, Seoul, Republic of Korea 04532 | Tel: +82-2-772-4000 | Fax: +82-2-772-4001/2 | E-mail: mail@leeko.com | www.leeko.com