Comparing privacy laws:
GDPR v. PIPL

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the authors

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

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

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

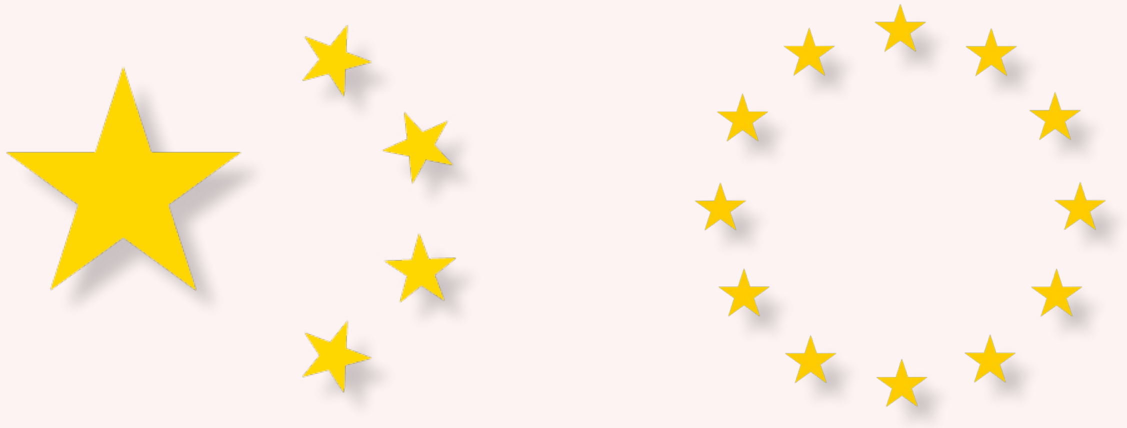
Contributors

OneTrust DataGuidance™
Angela Potter, Keshawna Campbell, Victoria Ashcroft

Image production credits:

Cover/p.5/p.51: cnythzl / Signature collection / istockphoto.com | MicroStockHub / Signature collection / istockphoto.com
Scale key p6-49: enisaksoy / Signature collection / istockphoto.com

Table of contents



Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect on 25 May 2018 and governs the protection of personal data in EU and EEA Member States. China's Personal Information Protection Law ('PIPL') was passed , on 20 August 2021 by the National People's Congress and is set to enter into effect 1 November 2021.

The PIPL is the first comprehensive data protection legislation in China and regulates personal information handling activities by personal information handlers and entrusted parties. The Cyberspace Administration of China ('CAC') has been appointed as the supervisory authority with individual departments at the local level also been afforded enforcement powers.

In general terms, there are broad similarities between the GDPR and the PIPL. The two legislations address matters such as data subject rights, provide lawful bases for data processing, and impose restrictions on international data transfers. Furthermore, the PIPL imposes similar responsibilities on data controllers with regards to the protection of personal data, including the appointment of a data protection officer ('DPO'), conducting Data Protection Impact Assessments ('DPIA'), and data breach reporting, although the PIPL uses different terminology. Nevertheless, the PIPL and the GDPR differ in some important respects, in particular, the PIPL allows the next of kin to exercise the rights of deceased persons and imposes personal liability for certain breaches of its provisions. Furthermore, the PIPL does not provide for data transfers based on adequate protection and establishes data localisation requirements for personal information handlers.

This overview organises provisions from the GDPR and the PIPL into key topics and sets them alongside each other to enable analysis and comparison. Each section begins with a detailing of principal information and a general introduction, as well as a consistency rating.

Structure and overview of the Guide

This Guide provides a comparison of the two legislative legal 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 legal frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the PIPL.

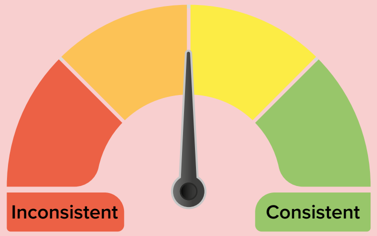
Key for giving the consistency rate

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

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

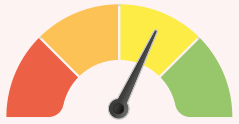
🟥 **Inconsistent:** The GDPR and the PIPL bear a high degree of difference with regard to the rationale, core, scope, and application of the provision considered.



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



Fairly consistent

1.1. Personal scope

The PIPL, similar to the GDPR, applies to individuals as well as private and state organs/ public bodies respectively. However, the PIPL differs from the GDPR in that it does not specify its applicability based on the nationality of the data subject nor does it state its applicability to deceased individuals, although it addresses the exercising of such persons' individual rights.

Furthermore, unlike the GDPR which provides a clear definition of data processors, the PIPL does not define entrusted parties. Nevertheless, both legislations outline requirements for such parties, with the GDPR requirements being more detailed.

GDPR	PIPL
Data controller	
Article 4(7): 'controller' means the natural or 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Article 73(1): 'Personal information handler' refers to an organisation or individual that, in personal information handling activities, determines autonomously the purposes and methods.
Data processor	
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	The PIPL does not explicitly define 'entrusted persons' but does outline requirements for the same in Article 21. In addition, Article 59 of the PIPL requires entrusted persons to take necessary measures to safeguard the security of personal information and assist the personal information handler in fulfilling its obligations under the PIPL.
Data subject	
Article 4(1): 'personal data' means 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.	Article 4: Personal information is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including anonymised information.

GDPR	PIPL
Public bodies	
Article 4(7): 'controller' means the natural or legal person, public authority, agency or other body.	Article 37: The provisions of the PIPL regarding personal information handling by State organs apply to the handling of personal information in the performance of statutory duties by organisations authorised by laws and regulations. [NB: Chapter 2, Section 3 of the PIPL establishes special provisions for the handling of personal information by State organs.]
Nationality of data subject	
Recital 14: The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.	The PIPL does not explicitly refer to the nationality of data subjects.
Place of residence	
See Recital 14, above.	The PIPL does not explicitly refer to the place of residence. However, Article 3 of the PIPL states that it applies to the handling the personal information of natural persons within the borders of the People's Republic of China.
Deceased individuals	
Recital 27: This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.	The PIPL does not explicitly address its applicability to deceased persons. However, Article 49 of the PIPL states that when a natural person dies, their next of kin may, for the sake of their own lawful, legitimate interests, exercise the rights provided in Chapter 4 to consult, copy, correct, delete, etc. the personal information of the deceased, except where the deceased has arranged otherwise before their death.

1.2. Territorial scope

Consistent

The GDPR and the PIPL bear many similarities in terms of territorial scope. In particular, the PIPL, analogous to the GDPR, has extraterritorial application, applying to personal information handlers that function outside of China in relation to the providing of products and services to natural persons and when analysing or assessing behaviour of natural persons.

Notably, the PIPL will also apply extraterritorially in other circumstances provided in laws or administrative regulations, where the GDPR does not contain a similar provision.

GDPR	PIPL
Establishment in jurisdiction	
Article 3: This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. Recital 22: Establishment implies the effective and real exercise of activity through stable arrangements.	Article 3: The PIPL applies to the activities of handling the personal information of natural persons within the borders of the People's Republic of China.
Extraterritorial	
See Article 3, above.	Article 3: The PIPL also applies in any of the following cases for the handling of personal information of natural persons in the People's Republic of China that is carried out outside of the People's Republic of China: • for the purpose of providing products or services to natural persons inside the territory; • to analyse or assess behaviour of natural persons inside the territory; and • in other circumstances provided in laws or administrative regulations.
Goods & services from abroad	
Recital 23: In order to ensure that natural persons are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union should be subject to this Regulation where the processing activities are related to offering goods or services to such data subjects irrespective of whether connected to a payment.	Please see Article 3 above.

GDPR	PIPL
Monitoring from abroad	
Recital 24: The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union should also be subject to this Regulation when it is related to the monitoring of the behaviour of such data subjects in so far as their behaviour takes place within the Union.	Please see Article 3 above.

1.3. Material scope

Fairly consistent

The PIPL and the GDPR adopt similar concepts of personal data, data processing, as well as pseudonymisation and anonymisation, referred to as 'de- identification' in the PIPL. In addition, both legislations provide general exceptions for the processing of personal data for purely personal or household activities and afford enhanced protection to special categories and sensitive data. The PIPL however, recognises the personal information of minors as sensitive data while the GDPR does not.

GDPR	PIPL
Personal data/ personal information	
Article 4(1): 'personal data' means 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.	Article 4: Personal information is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including anonymised information..
Data processing	
Article 4(2): 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, 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.	Article 4: Personal information handling includes personal information collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.
Special categories of data	
Article 9(1): Processing of 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 a natural person's sex life or sexual orientation shall be prohibited.	Article 28: Sensitive personal information means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.
Anonymised data	
Recital 26: The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to	Article 4 specifies that anonymised information is not to be considered personal information.

GDPR	PIPL
Anonymised data (cont'd)	
personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	Article 73(4): Anonymisation refers to the process by which personal information is handled to make it impossible to distinguish specific natural persons and impossible to restore.
Pseudonymised data	
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data 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.	Article 73(3): De-identification refers to the process by which personal information is handled so that a natural person cannot be identified without additional information.
Automated processing	
Article 2(1): This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.	Article 4: Personal information is all kinds of information, recorded by electronic or other means [...].
General exemptions	
Article 2(2): This Regulation does not apply to the processing of personal data: a. in the course of an activity which falls outside the scope of Union law; b. by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; or c. by a natural person in the course of a purely personal or household activity.	Article 72: The PIPL does not apply to natural persons handling personal information for personal or family affairs.

2. Key definitions

2.1. Personal data

The PIPL and GDPR both provide definitions of personal data and sensitive/special categories of personal information, respectively. However, unlike the GDPR, the PIPL does not define online identifiers, health, biometric, and genetic data, among other concepts. In addition, unlike the GDPR, the PIPL recognises the personal information of minors as sensitive data.

GDPR	PIPL
Personal data/personal information	
Article 4(1): 'personal data' means 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.	Article 4: Personal information is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including anonymised information.
Special categories of data	
Article 9(1): Processing of 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 a natural person's sex life or sexual orientation shall be prohibited.	Article 28: Sensitive personal information means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.
Online identifiers	
Recital 30: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.	The PIPL does not explicitly refer to online identifiers.
Others	
Not applicable.	Not applicable.

2.2. Pseudonymisation

Consistent

The PIPL and GDPR provide a definition for the anonymisation and pseudonymisation/ de-identification of personal information. In addition, both the GDPR and the PIPL require the implementation of technical and organisational measures to ensure that personal data is not attributable to a data subject.

GDPR	PIPL
Anonymisation	
Recital 26: 'anonymous information' is information which 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.	Article 73(4): Anonymisation refers to the process by which personal information is handled to make it impossible to distinguish specific natural persons and impossible to restore.
Pseudonymisation	
Article 4(5): 'pseudonymisation' means the processing of personal data in such a manner that the personal data 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.	Article 73(3): De-identification refers to the process by which personal information is handled so that a natural person cannot be identified without additional information. Article 51: Personal information handlers shall, on the basis of the personal information handling purpose, handling methods, personal information categories, as well as the influence on individuals' rights and interests, possibly existing security risks, etc adopt the following measures [...] corresponding technical security measures such as encryption, de-identification, etc.

2.3. Controllers and processors

Fairly consistent

The PIPL and the GDPR both provide definitions of personal information handler and data controller, respectively and require the execution of a contract between the same. In addition, both legislations require the conducting of DPIAs/Personal information Protection Impact Assessments ('PIPIA') and the appointment of a DPO/personal information protection officer ('PIPO') in certain circumstances. However, unlike the GDPR the PIPL does not provide a definition of entrusted parties.

GDPR	PIPL
Data controller	
Article 4(7): 'controller' means the natural or 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.	Article 73(1): 'Personal information handler' refers to an organisation or individual that, in personal information handling activities, determines autonomously the purposes and methods.
Data processor	
Article 4(8): 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.	The PIPL does not explicitly define 'entrusted persons' but does outline requirements for the same in Article 21.
Controller and processor contracts	
Article 28(3): Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. [Article 28 goes on to stipulate necessary information to be included in such a contract.]	Article 21: Where personal information handlers entrust the handling of personal information, they shall conclude an agreement with the entrusted person on the purpose, duration, and manner of the entrusted handling, categories of personal information, protection measures, as well as the rights and duties of both sides, etc., and conduct supervision of the personal information handling activities of the entrusted person. Entrusted persons shall handle personal information according to the agreement and shall not handle personal information beyond the agreed purpose and manner of processing. If the entrusting contract does not take effect, is void, has been cancelled, or has been terminated, the entrusted person shall return the personal information to the personal information handler or delete it, and may not retain it. Without the consent of the personal information handler, the entrusted person may not entrust

GDPR	PIPL

Controller and processor contracts (cont'd)

GDPR	PIPL
	others to handle personal information. [NB: Although the PIPL does not specific specifica obligations for entrusted persons, Article 59 of the PIPL requires entrusted persons to take necessary measures to safeguard the security of personal information and assist the personal information handler in fulfilling its obligations under the PIPL.]

Data Protection Impact Assessment ('DPIA')

GDPR	PIPL
DPIA is not specifically defined, however Article 35 sets out requirements for DPIAs (see section 5.3. for further information).	PIPIA is not specifically defined, however Articles 55 and 56 of the PIPL sets out requirements for PIPIAs (see section 5.3. below for further information).

Data Protection Officer ('DPO')

GDPR	PIPL
DPO is not specifically defined, however Article 37 sets out requirements related to DPOs (see section 5.4. for further information).	PIPO is not specifically defined, however Article 52 of the PIPL sets out requirements related to PIPOs (see section 5.4. below for further information).

2.4. Children

Fairly consistent

The GDPR and the PIPL address the processing of childrens'/minors' personal data and require consent from their parent/guardian or legal representative to process such personal information. Notably, the GDPR outlines requirements for privacy notices aimed at children, while the PIPL requires the development of special rules for the handling of minors' personal information.

GDPR	PIPL

Children's definition

GDPR	PIPL
The GDPR does not specifically define 'child'. However, Article 8(1) provides: Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.	The PIPL does not specifically define 'minor.' However, as part of the definition of 'sensitive personal information' under Article 28 of the PIPL and the obligations under Article 31 of the PIPL, the PIPL refers to minors under the age of 14.

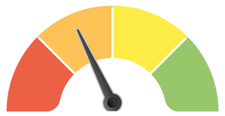
Consent for processing children's data

GDPR	PIPL
Article 8(2): The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.	Article 31(1): Where personal information handlers handle the personal information of minors under the age of 14, they shall obtain the consent of the parent or other guardian of the minor. Where a personal information handler handles personal information of a minor under the age of 14, special handling rules shall be formulated. [NB: Article 28 of the PIPL also classifies the personal information of minors under the age of 14 as 'sensitive personal information.' Accordingly, pursuant to Article 29 of the PIPL, to handle sensitive personal information, the individual's separate consent shall be obtained. Where laws or administrative regulations provide that written consent shall be obtained for handling sensitive personal information, those provisions are to be followed.]

Privacy notice (children)

GDPR	PIPL
Recital 58: Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.	The PIPL does not explicitly refer to privacy notices for children.

2.5. Research


Fairly inconsistent

The GDPR unlike the PIPL permits personal data to be processed for scientific research purposes including historical, archiving, or statistical purposes and provides limitations on data subject rights in specific circumstances when processing for these purposes. Both legislations, nevertheless, allow for the further processing of personal information for purposes compatible with the original purpose of collection in certain circumstances.

GDPR	PIPL
Scientific/historical research definition	
Recital 159: Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, 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. Recital 160: Where personal data are processed for historical research purposes, this Regulation should also apply to that processing. This should also include historical research and research for genealogical purposes, bearing in mind that this Regulation should not apply to deceased persons.	The PIPL does not specifically define research purposes. However, Article 72 of the PIPL clarifies that where the law provides for the handling of personal information by governments at various levels and their relevant departments in implementing statistical and archival management activities, those provisions apply.
Compatibility with original purpose of collection	
Article 5(1)(b): Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; 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 ('purpose limitation').	Article 27: Personal information handlers may, within a reasonable scope, handle personal information that has already been disclosed by the person themselves or otherwise lawfully disclosed, except where the person clearly refuses. Personal information handlers handling already disclosed personal information, where there is a major influence on individual rights and interests, shall obtain personal consent in accordance with the provisions of the PIPL. [NB: More generally, Article 6 of the PIPL provides that the handling of personal information shall have a clear and reasonable purpose and shall be directly related to the purpose in such a way as to have minimal impact on the interests of individuals. Furthermore, the collection of personal information shall be limited to the smallest extent possible to achieve the purpose and not be excessive. Finally, pursuant to Article 14 of the PIPL, where the handling of information is based on consent, consent must be obtained if the purpose, manner, and type of handling changes.]
Appropriate safeguards	
Article 89(1): Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner.	The PIPL does not directly address this matter.
Data subject rights (research)	
Under Article 17(3), the right to erasure may not apply in cases of scientific or historical research. Article 21(6), however, provides that data subjects may exercise the right to object to data processing for scientific or historical research purposes. In addition, Article 89 provides that Member States may derogate from the GDPR in regard to data subject rights and data processing for research purposes.	The PIPL does not directly address this matter.

3. Legal basis

Fairly consistent

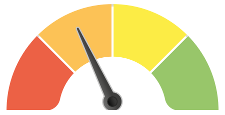
The PIPL and GDPR outline grounds for the lawful processing of personal information. Notably, the GDPR provides for personal information to be processed on the bases of the legitimate interest of the data controller, whereas the PIPL does not contain a similar provision. Further to this, both legislations provide detailed requirements for valid consent from data subjects and expressly provide data subjects with a right to withdraw consent at any time.

GDPR	PIPL
Legal grounds	
Article 6(1): Processing shall be lawful only if and to the extent that at least one of the following applies: • the data subject has given consent to the processing of his or her personal data for one or more specific purposes; • processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; • processing is necessary for compliance with a legal obligation to which the controller is subject; • processing is necessary in order to protect the vital interests of the data subject or of another natural person; • processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or • processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.	Article 13: Personal information handlers may only handle personal information where they conform to one of the following circumstances: • obtaining individuals' consent; • where necessary to conclude or fulfil a contract in which the individual is an interested party, or where necessary to conduct human resources management in accordance with lawfully formulated labour rules and structures and lawfully concluded contracts; • where necessary to fulfil statutory duties and responsibilities or statutory obligations; • where necessary to respond to sudden public health incidents, or protect natural persons' lives and health or the security of their property, under emergency conditions; • handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest; • when handling personal information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of the PIPL; and • in other circumstances provided in laws and administrative regulations.
Sensitive data (legal basis)	
There are specific requirements for processing special categories of data, see Article 9 of the GDPR for further information.	There are specific requirements for the handling of sensitive personal information, see Articles 28 to 32 of the PIPL for further information.

GDPR	PIPL
Conditions for consent	
Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. Article 4: (11) 'consent' of the data subject means 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.	Article 14: Where personal information is handled based on individual consent, said consent shall be given by individuals under the precondition of full knowledge, and in a voluntary and explicit statement. Where laws or administrative regulations provide that separate consent or written consent shall be obtained to handle personal information, those provisions are to be followed. If the purpose, manner, and type of handling changes, personal consent shall be obtained again. Article 15: Where personal information is handled based on individual consent, individuals have the right to rescind their consent. Personal information handlers shall provide a convenient way to withdraw consent. If an individual rescinds consent, it does not affect the effectiveness of personal information handling activities undertaken on the basis of individual consent before consent was rescinded. Article 16: Personal information handlers may not refuse to provide products or services on the basis that an individual does not consent to the handling of their personal information or rescinds their consent, except where handling personal information is necessary for the provision of products or services.
Journalism/artistic purposes	
Article 85(1): Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.	Article 13(5): Personal information handlers may only handle personal information where they conform to one of the following circumstances [...] handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest.

4. Controller and processor obligations

4.1. Data transfers



Fairly inconsistent

The GDPR provides for the cross-border transfer of personal information based on adequate protection, while the PIPL does not. The PIPL and GDPR however, outline mechanisms including contractual clauses to enable international data transfers. Further to this, the PIPL outlines data localisation requirements, while the GDPR does not contain an equivalent provision.

Adequate protection

GDPR	PIPL
Article 45(1): A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.	The PIPL does not explicitly address data transfers based on adequate protection. However, generally, Article 38 of the PIPL stipulates that the personal information handler shall take necessary measures to ensure that the activities of the foreign receiving party in handling personal information meet the standards for the protection of personal information set forth in this Law.

Other mechanisms for data transfers

GDPR	PIPL
Article 46(1): In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by: • a legally binding and enforceable instrument between public authorities or bodies; • binding corporate rules in accordance with Article 47; • standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);	Article 38: Where personal information handlers are required to provide personal information outside the territory of the People's Republic of China for business or other such requirements, they shall meet one of the following conditions: • passing a security assessment organised by the CAC according to Article 40 of the PIPL; • undergoing personal information protection certification conducted by a specialised body according to provisions by the CAC; • concluding a contract with the foreign receiving party in accordance with a standard contract formulated by CAC, agreeing upon the rights and responsibilities of both sides; and • in other conditions provided in laws or administrative regulations or by the CAC.

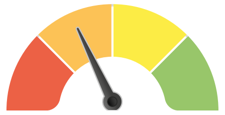
Other mechanisms for data transfers (cont'd)

GDPR	PIPL
• standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2); • an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or • an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights. Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided for, in particular, by: • contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or • provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.	[NB: According to Article 38 of the PIPL, international treaties and agreements concluded or acceded to by the People's Republic of China may be implemented in accordance with its provisions on the conditions for the provision of personal information outside the territory of the People's Republic of China.]

Data localisation

GDPR	PIPL
Not applicable.	Article 40: Critical information infrastructure operators and personal information handlers handling personal information reaching quantities provided by the CAC shall store personal information collected and produced within the borders of the People's Republic of China domestically. Where they need to provide it abroad, they shall pass a security assessment organised by the CAC; where laws or administrative regulations and CAC provisions permit that security assessment not be conducted, those provisions are to be followed.

4.2. Data processing records


Fairly inconsistent

While the GDPR requires both data controllers and data processors to maintain a record of their data processing activities, the PIPL only imposes such requirements on personal information handlers when processing certain types of personal information. In addition, the GDPR outlines a limited number of exemptions to the requirement, whereas the PIPL does not.

Data controller obligation

GDPR	PIPL
Article 30(1): Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: • the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; • the purposes of the processing; • a description of the categories of data subjects and of the categories of personal data; • the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; • where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; • where possible, the envisaged time limits for erasure of the different categories of data; and • where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	Article 55: When one of the following circumstances is present, personal information handlers shall [...] record the handling: • handling sensitive personal information; • using personal information to conduct automated decision-making; • entrusting personal information handling, providing personal information to other personal information handlers, or disclosing personal information; • providing personal information abroad; and • other personal information handling activities with a major influence on individuals.

Data processor obligation

GDPR	PIPL
Article 30(2): Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing: • the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer; • the categories of processing carried out on behalf of each controller;	The PIPL does not contain specific record-keeping requirements for data processors. [NB: Although the PIPL does not specify specific obligations for entrusted persons, Article 59 of the PIPL requires entrusted persons to take necessary measures to safeguard the security of personal information and assist the personal information handler in fulfilling its obligations under the PIPL.]

Data processor obligation (cont'd)

GDPR	PIPL
• where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; and • where possible, a general description of the technical and organisational security measures referred to in Article 32(1).	

Records format

GDPR	PIPL
Article 30(3): The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.	The PIPL does not explicitly address format of records.

Required to make available

GDPR	PIPL
Article 30(4): The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.	The PIPL does not explicitly require records to be made available. However, Article 56 of the PIPL outlines that records shall be preserved for at least three years. In this regard, pursuant to Article 63(2) of the PIPL, departments responsible for the protection of personal information may inspect and copy records relating to the handling of personal information (see section 6.2. below for further information).

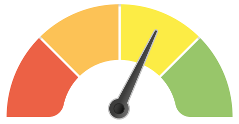
Exemptions

GDPR	PIPL
Article 30(5): The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.	The PIPL does not explicitly address exemptions for record-keeping requirements.

General Data Processing Notification ('DPN')

GDPR	PIPL
Not applicable.	Not applicable.

4.3. Data protection impact assessment

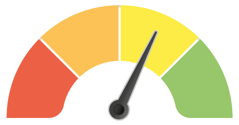


Fairly consistent

The GDPR and PIPL contain similar provisions regarding DPIAs and PIPIAs, respectively. In particular, both legislations outline requirements for when an assessment must be conducted and the content of such assessments. Nevertheless, the GDPR requires prior consultation with the data protection authority in specific circumstances, whereas the PIPL does not.

GDPR	PIPL
When is a DPIA required	
Article 35(1): Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. [...] (3) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: • a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; • processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or • a systematic monitoring of a publicly accessible area on a large scale.	Article 55: When one of the following circumstances is present, personal information handlers shall conduct a PIPIA in advance [...]: • handling sensitive personal information; • using personal information to conduct automated decision-making; • entrusting personal information handling, providing personal information to other personal information handlers, or disclosing personal information; • providing personal information abroad; and • other personal information handling activities with a major influence on individuals
DPIA content requirements	
Article 35(7): The assessment shall contain at least: • a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; • an assessment of the necessity and proportionality of the processing operations in relation to the purposes; • an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and	Article 56: The content of the PIPIA shall include: • whether or not the purpose and manner of handling personal information are lawful, legitimate, and necessary; • the impact on individuals' rights and interests, and the security risks; and • whether protective measures undertaken are legal, effective, and suitable to the degree of risk. [NB: According to Article 56 of the PIPL, PIPIA reports must be preserved for at least three years.]
DPIA content requirements (cont'd)	
• the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	
Consultation with authority	
Article 36(1): The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk. [Article 36 goes on to detail requirements related to such prior consultation].	The PIPL does not explicitly address consultation with authorities. However, pursuant to Article 63(2) of the PIPL, departments responsible for the protection of personal information may inspect and copy all relevant materials relating to the handling of personal information (see section 6.2. below for further information).

4.4. Data protection officer appointment



The PIPL provides for the appointment of a PIPO, similar to the DPO requirement under the GDPR. Specifically, both laws outline the responsibilities of such individuals and requires that DPOs and PIPOs be reported to the relevant authority. However, the GDPR outlines the qualifications of such persons and allows for the appointment of a single DPO or responsible person for group undertakings, while the PIPL is silent on these matters.

GDPR	PIPL
DPO tasks	
Article 39(1): The data protection officer shall have at least the following tasks: • to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; • to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or 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; • to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35; • to cooperate with the supervisory authority; and • to act as the contact point for 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.	Article 52: Personal information handlers that handle personal information reaching quantities provided by the CAC shall appoint PIPO, to be responsible for supervising personal information handling activities as well as adopted protection measures, etc.
When is a DPO required	
Article 37(1): The controller and the processor shall designate a data protection officer 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 the controller or the processor 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 consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offenses referred to in Article 10.	Please see Article 52(1) above.
Group appointments	
Article 37(2): A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.	The PIPL does not explicitly address group appointments for PIPO.
Notification of DPO	
Article 37(7): The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.	Article 52: Personal information handlers shall disclose the methods of contacting PIPO, and report the personal names of the officers and contact methods to the departments responsible for the protection of personal information.
Qualifications	
Article 37(5): The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.	The PIPL does not explicitly address PIPO qualifications.

4.5. Data security and data breaches

Fairly consistent

The PIPL and the GDPR both contain provisions regarding security measures that should be implemented by controllers and personal information handlers. In particular, both legislations require data breaches to be notified to the relevant supervisory authority in specific circumstances and details the content of such notifications.

In addition, the PIPL similar to the GDPR, provides exceptions to data breach notification requirements where the personal information handler is able to adopt measures that are able to effectively avoid harm created by information leak, distortion, or loss.

Security measures defined

GDPR	PIPL
Article 32(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: • 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 the availability and access to personal data in a timely manner in the event of a physical or technical incident; • a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	Article 51: Personal information handlers shall take the following measures to ensure that personal information handling activities comply with the provisions of laws and administrative regulations and to prevent unauthorised access, disclosure, tampering with, or loss of personal information, according to the purpose and manner of handling, the type of personal information, and the impact on individuals' rights and interests: • formulating internal management structures and operating rules; • implementing categorised management of personal information; • adopting corresponding technical security measures such as encryption, de-identification, etc.; • reasonably determining operational limits for personal information handling, and regularly conducting security education and training for employees; • formulating and organising the implementation of personal information security incident response plans; and • other measures provided in laws or administrative regulations.

Data breach notification to authority

GDPR	PIPL
Article 33(1): In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.	Article 57: Where a personal information leak, distortion, or loss occurs or might have occurred, personal information handlers shall immediately adopt remedial measures, and notify the departments responsible for the protection of personal information and the individuals. The notification shall include the following: • the types of information, causes and possible hazards caused by the disclosure, tampering, or loss of personal information; • remedial measures taken by personal information handlers and mitigation measures that may be taken by individuals; and • contact information for personal information handles.

Data breach notification to authority (cont'd)

Timeframe for breach notification

GDPR	PIPL
See Article 33(1) above.	See Article 57 above.

Notifying data subjects of data breach

GDPR	PIPL
Article 34(1): When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	See Article 57 above.

Data processor notification of data breach

GDPR	PIPL
Article 33(2): The processor shall notify the controller without undue delay after becoming aware of a personal data breach.	The PIPL does not explicitly address data breaches reporting by data processors. [NB: Although the PIPL does not specify specific obligations for entrusted persons, Article 59 of the PIPL requires entrusted persons to take necessary measures to safeguard the security of personal information and assist the personal information handler in fulfilling its obligations under the PIPL.]

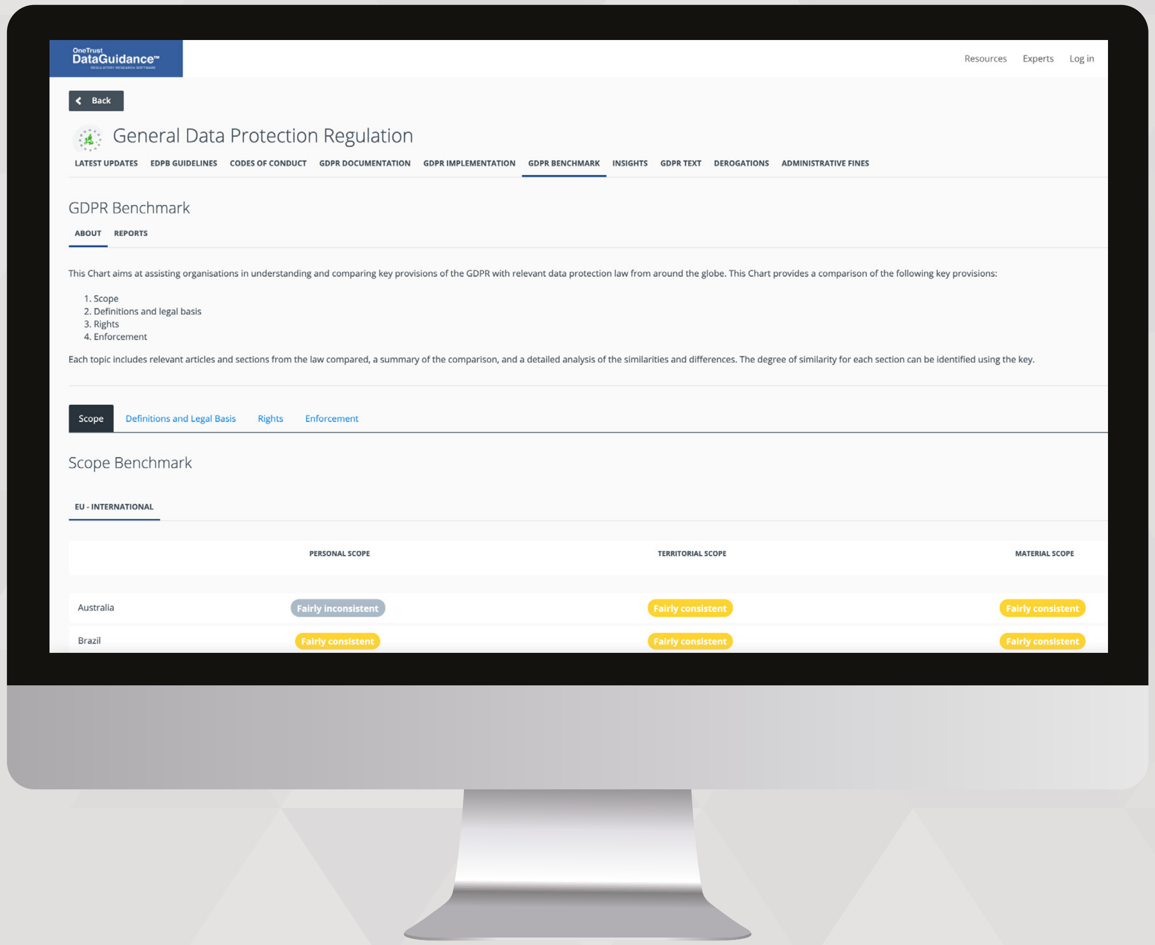
Data processor notification of data breach

GDPR	PIPL
Article 34(3): The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: a. the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; b. the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; and c. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.	Article 57: Where personal information handlers adopt measures that are able to effectively avoid harm created by information leaks, distortion, or loss, personal information handlers are permitted to not notify individuals; however, where departments responsible for the protection of personal information believe harm may have been created, they may require personal information handlers to notify individuals.

Global Regulatory Research Software

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

Monitor regulatory developments, mitigate risk, and achieve global compliance



General Data Protection Regulation

GDPR Benchmark

This Chart aims at assisting organisations in understanding and comparing key provisions of the GDPR with relevant data protection law from around the globe. This Chart provides a comparison of the following key provisions:

1. Scope
2. Definitions and legal basis
3. Rights
4. Enforcement

Each topic includes relevant articles and sections from the law compared, a summary of the comparison, and a detailed analysis of the similarities and differences. The degree of similarity for each section can be identified using the key.

Scope Benchmark

	PERSONAL SCOPE	TERRITORIAL SCOPE	MATERIAL SCOPE
Australia	Fairly inconsistent	Fairly consistent	Fairly consistent
Brazil	Fairly consistent	Fairly consistent	Fairly consistent

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

OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Start your free trial at
www.dataguidance.com

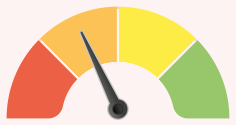
4.6. Accountability

Fairly consistent

The PIPL does not contain an express principle of accountability, as is the case in the GDPR. However, the PIPL requires personal information handlers to accept responsibility for their personal information handling activities and to adopt the measures necessary to safeguard the security of the personal information they handle.

GDPR	PIPL
Principle of accountability	
Article 5(2): The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). [Paragraph 1 details principles of: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality.]	The PIPL does not contain a specific provision for the principle of accountability. However, Article 9 of the PIPL states: Personal information handlers shall bear responsibility for their personal information handling activities and adopt the necessary measures to safeguard the security of the personal information they handle.
Liability of data controllers and data processors	
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.	Article 20: A person who jointly handles personal information and infringes upon the rights and interests of personal information shall bear joint and several liability in accordance with law. Article 59: Entrusted persons shall, in accordance with the provisions of the PIPL and the relevant laws and administrative regulations, take the necessary measures to safeguard the security of the personal information processed and assist the personal information processor in fulfilling its obligations under the PIPL. Article 69: If the handling of personal information infringes upon the rights and interests of personal information and causes damage, and the personal information handler cannot prove they are not at fault, they shall bear the liability for damages and compensation.

5. Rights


Fairly inconsistent

5.1. Right to erasure

The GDPR and the PIPL provide a right to erasure and deletion, respectively. In terms of the right to erasure, both legislations provide grounds and exceptions for exercising this right including the withdrawal of consent and personal data having been unlawfully processed. Nevertheless, the GDPR outlines a clear timeframe and format for responding to such requests, whereas the PIPL requires personal information handlers to be proactive about such requests.

Furthermore, GDPR unlike the PIPL, requires data controllers to notify other parties, with whom the information may have been shared, about a request.

GDPR	PIPL
Grounds for erasure	
Article 17(1): The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: • the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; • the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; • the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); • the personal data have been unlawfully processed; • the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; and • the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).	Article 47: Personal information handlers shall proactively delete personal information where one of the following circumstances occurs; if the personal information handler has not deleted it, individuals have the right to request deletion: • the handling purpose has been achieved, is impossible to achieve, or [the personal information] is no longer necessary to achieve the handling purpose; • personal information handlers cease the provision of products or services, or the retention period has expired; • the individual rescinds consent; • personal information handlers handled personal information in violation of laws, administrative regulations, or agreements; or • other circumstances provided by laws or administrative regulations.
Inform data subject of right	
Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain	The PIPL does not explicitly address whether individuals must be informed of the right to erasure. However, Article 17 of the PIPL states that personal information handlers shall, before handling personal

Inform data subject of right (cont'd)

GDPR	PIPL
language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	information, explicitly notify individuals truthfully, accurately, and fully of the following items using clear and easily understood language the methods and procedures for individuals to exercise the rights provided in the PIPL.

Fees

GDPR	PIPL
Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: • charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or • refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	The PIPL does not refer to fees in relation to the right to erasure.

Response timeframe

GDPR	PIPL
Article 12(3): The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.	Article 47(1): Personal information handlers shall proactively delete personal information where one of the following circumstances occurs [...]

Format of response

GDPR	PIPL
Article 12(1): The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	The PIPL does not refer to the format of a response in relation to the right to erasure. However, Article 50 of the PIPL states personal information handlers shall establish convenient mechanisms to accept and handle applications from individuals to exercise their rights. Where they reject individuals' requests to exercise their rights, they shall explain the reason.

Publicly available data

GDPR	PIPL
Article 17(2): Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.	The PIPL does not explicitly address publicly available data. [NB: Article 27 of the PIPL establishes additional provisions for personal information disclosed by the individual (see section 2.5. for further information).]

Exceptions

GDPR	PIPL
Article 17(3): Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: • for exercising the right of freedom of expression and information; • for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; • for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); • for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or • for the establishment, exercise or defence of legal claims.	Article 47: Where the retention period provided by laws or administrative regulations has not expired, or personal information deletion is technically hard to realise, personal information handlers shall cease personal information handling except for storage and taking necessary security protective measures.

GDPR	PIPL
Exceptions (cont'd)	
Article 12(5): Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: • charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or • refuse to act on the request. The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request. Article 47: Where the retention period provided by laws or administrative regulations has not expired, or personal information deletion is technically hard to realise, personal information handlers shall cease personal information handling except for storage and taking necessary security protective measures.	

5.2. Right to be informed

Fairly consistent

The GDPR and the PIPL provide requirements for data controllers to notify data subjects when collecting and processing their personal information. In particular, both pieces of legislation outline what information must be disclosed, detail when such information must be shared, and provide exceptions to this right. However, the GDPR, unlike the PIPL, differentiates between information collected directly from the individual and information obtained from third parties.

GDPR	PIPL
Informed prior to/at collection	
Article 13(1): Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: • the identity and the contact details of the controller and, where applicable, of the controller's representative; • the contact details of the data protection officer, where applicable; • the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; • where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; • 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 or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing: • the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; • the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to	Article 17: Personal information handlers shall, before handling personal information, explicitly notify individuals truthfully, accurately, and fully of the following items using clear and easily understood language: • the name or personal name and contact method of the personal information handler; • the purpose of personal information handling and the handling methods, the categories of handled personal information, and the retention period; • methods and procedures for individuals to exercise the rights provided in the PIPL; and • other matters to be communicated under laws or administrative regulations.

Informed prior to/at collection (cont'd)

GDPR	PIPL
object to processing as well as the right to data portability; • where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; • the right to lodge a complaint with a supervisory authority; • whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	

What information is to be provided

GDPR	PIPL
See Article 13(1) and (2) above.	See Article 17 above. Article 23: Where a personal information handler provides personal information to other personal information handlers, they shall notify the name and contact details of the recipient, the purpose and method of handling, and the type of personal information [...] Article 30: Personal information handlers handling sensitive personal information, in addition to the items set out in Paragraph 1 of Article 17 of the PIPL, shall also notify individuals of the necessity and influence on the individual's rights and interests of handling the sensitive personal information, except where the PIPL provides that it is permitted not to notify the individuals. Article 48: Individuals have the right to request personal information handlers explain personal information handling rules.

When data is from third party

GDPR	PIPL
In addition to the information required under Article 13, Article 14(2) replaces the requirement that data subjects are provided with information on the legitimate interests pursued by the controller or by a third party, with an obligation to inform data subjects of the categories of personal data. Furthermore, paragraph (e) of Article 13(2) is replaced with a requirement to inform data subjects of the source from which the personal data originate, and if applicable, whether it came from publicly accessible sources.	The PIPL does not specifically address the right to be informed when data is obtained from a third party. More generally, see Article 27 above.

Intelligibility requirements

GDPR	PIPL
Article 12(1): The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	Article 17: Personal information handlers shall, before handling personal information, explicitly notify individuals truthfully, accurately, and fully [...] using clear and easily understood language.

Format

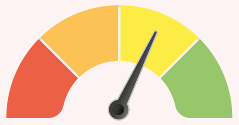
GDPR	PIPL
See Article 12(1) above.	Article 17: Where personal information handlers notify the matters as provided in Paragraph 1 of Article 17 of the PIPL through the method of formulating personal information handling rules, the handling rules shall be made public [disclosed] and convenient to read and store.

Exceptions

GDPR	PIPL
The requirements of Article 13 do not apply where the data subject already has the information. The requirements of Article 14 do not apply where: • the data subject already has the information; • the provision of such information proves impossible	Article 18: Personal information handlers handling personal information are permitted not to notify individuals about the items provided Paragraph 1 of Article 17 of the PIPL under circumstances where laws or administrative regulations provide that confidentiality shall be preserved or notification is not necessary.

GDPR	PIPL
Exceptions (cont'd)	
in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in Article 89(1) or in so far as the obligation referred to in paragraph 1 of this Article is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available; • obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or • where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.	Under emergency circumstances, where it is impossible to notify individuals in a timely manner in order to protect natural persons' lives, health, and the security of their property, personal information handlers shall notify them after the conclusion of the emergency circumstances. Article 30: Personal information handlers handling sensitive personal information, in addition to the items set out in Paragraph 1 of Article 17 of the PIPL, shall also notify individuals of the necessity and influence on the individual's rights and interests of handling the sensitive personal information, except where the PIPL provides that it is permitted not to notify the individuals.

5.3. Right to object


Fairly consistent

Similar to the right to object under the GDPR, the PIPL provides a right to refuse the handling of his/her personal information, in particular, in relation to personal information processed for direct marketing purposes. In addition, both pieces of legislation provide data subjects with a right to restrict the processing or to limit the use of their personal information and provide an explicit right to withdraw consent at any time.

However, the PIPL does not address whether individuals must be informed of this right, the payment of fees, or timeframes for responding to such requests.

GDPR	PIPL
Grounds for right to object/ opt out	
Article 21(1): The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.	Article 44: Individuals [...] have the right to limit or refuse the handling of their personal information by others, unless laws or administrative regulations stipulate otherwise.
Withdraw consent	
Article 7(3): The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	Article 15: Where personal information is handled based on individual consent, individuals have the right to rescind their consent. Personal information handlers shall provide a convenient way to withdraw consent.
Restrict processing	
Article 18(1): The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: • the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; • the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;	See Article 44 above.

Restrict processing (cont'd)

GDPR	PIPL
• the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; • the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.	

Object to direct marketing

GDPR	PIPL
Article 21(3): Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.	Article 24: Those conducting information push delivery or commercial sales to individuals through automated decision-making methods shall simultaneously provide the option to not target an individual's characteristics, or provide the individual with a convenient method to refuse.

Inform data subject of right

GDPR	PIPL
See Article 12(1) in section 6.1. above. In addition, Article 21(4) provides: At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.	The PIPL does not explicitly address whether individuals must be informed of the right to be informed. However, Article 17 of the PIPL states that personal information handlers shall, before handling personal information, explicitly notify individuals truthfully, accurately, and fully of the following items using clear and easily understood language the methods and procedures for individuals to exercise the rights provided in the PIPL.

Fees

GDPR	PIPL
See Article 12(5) in section 6.1. above.	The PIPL does not refer to fees in relation to the right to object.

Response timeframe

GDPR	PIPL
See Article 12(3) in section 6.1. above.	The PIPL does not explicitly address timeframe for responses.

Format of response

GDPR	PIPL
See Article 12(1) in section 6.1. above.	The PIPL does not explicitly impose a format of response. However, Article 50 of the PIPL states personal information handlers shall establish convenient

Format of response (cont'd)

GDPR	PIPL
	mechanisms to accept and handle applications from individuals to exercise their rights. Where they reject individuals' requests to exercise their rights, they shall explain the reason.

Exceptions

GDPR	PIPL
See Article 12(5) in section 6.1. above.	The PIPL does not explicitly provide any exceptions to the right to limit or refuse the handling of their personal information.

5.4. Right of access

Fairly consistent

Similar to the GDPR's right to access, the PIPL provides a right to consult and copy. Specifically, both legislations provide data subject with a right to obtain information about his/her personal information that is being processed. Unlike the PIPL, the GDPR outlines the information that must be provided to the data subject upon request. Furthermore, the PIPL does not address whether verification is required.

GDPR	PIPL
Grounds for right of access	
Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed.	Article 45: Individuals have the right to consult and copy their personal information from personal information handlers [...]
Information to be accessed	
Article 15(1): The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: • the purposes of the processing; • the categories of personal data concerned; • the recipients or categories of recipient to whom the personal data have 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, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	See Article 45 above.

GDPR	PIPL
Inform data subject of right	
See Article 12(1) in section 6.1.	The PIPL does not explicitly address whether individuals must be informed of the right to access. However, Article 17 of the PIPL states that personal information handlers shall, before handling personal information, explicitly notify individuals truthfully, accurately, and fully of the following items using clear and easily understood language the methods and procedures for individuals to exercise the rights provided in the PIPL.
Fees	
See Article 12(5) in section 6.1. above.	The PIPL does not refer to fees in relation to the right to access.
Verify data subject request	
Recital 64: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.	The PIPL does not address verification requirements for access requests.
Response timeframe	
See Article 12(3) in section 6.1. above.	Article 45(2): Where individuals request to consult or copy their personal information, personal information handlers shall provide it in a timely manner.
Format of Response	
See Article 12(1) in section 6.1. above.	The PIPL does not explicitly impose a format of response. However, Article 50 of the PIPL states personal information handlers shall establish convenient mechanisms to accept and handle applications from individuals to exercise their rights. Where they reject individuals' requests to exercise their rights, they shall explain the reason.
Format of Response	
See Article 12(5) in section 6.1. above.	Article 45(1): Individuals have the right to consult and copy their personal information from personal information handlers, except in circumstances provided in Paragraph 18 of Article 18 or Article 35 of the PIPL.

5.5. Right not to be subject to discrimination

Consistent

Similar to the GDPR, the right not to be subject to discrimination in exercising rights is not explicitly mentioned in the PIPL. However, under both legislations such a right can be inferred based on the protection from adverse effects on individuals' personal rights and interests. In addition, the GDPR and PIPL provide a right to object to automated processing.

GDPR	PIPL
Definition of right	
The GDPR only implies this right and does not provide an explicit definition for it.	The PIPL only implies this right and does not provide an explicit definition for it.
Automated processing	
Article 22(1): The 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 him or her or similarly significantly affects him or her. [Article 22 goes on to detail this right, including exceptions]	Article 24: When the use of automated decision-making produces decisions with a major influence on the rights and interests of the individual, they have the right to require personal information handlers to explain the matter, and they have the right to refuse that personal information handlers make decisions solely through automated decision-making methods.

5.6. Right to data portability

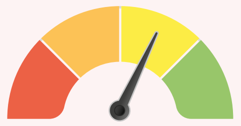
Fairly consistent

The GDPR and the PIPL both recognise a right to data portability. Nevertheless, the GDPR clarifies the instance when data subjects can exercise this right and whether fees can be charged, while the PIPL is silent on the matter.

GDPR	PIPL
Grounds for portability	
Article 20(1): The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where: • the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and • the processing is carried out by automated means.	Article 45: Where individuals request that their personal information be transferred to a personal information handler they designate, meeting conditions of the CAC, personal information handlers shall provide a channel to transfer it.
Inform data subject of right	
See Article 12(1) in section 6.1.	The PIPL does not explicitly address whether individuals must be informed of the right to data portability. However, Article 17 of the PIPL states personal information handlers shall, before handling personal information, explicitly notify individuals truthfully, accurately, and fully of the following items using clear and easily understood language [...] methods and procedures for individuals to exercise the rights provided in this Law.
Fees	
See Article 12(5) in section 6.1. above.	The PIPL does not refer to fees in relation to the right to data portability.
Response timeframe	
See Article 12(3) in section 6.1. above.	The PIPL does not explicitly address timeframe for responses.
Format	
See Article 20(1) above.	The PIPL does not explicitly impose a format of response.

GDPR	PIPL
Format (cont'd)	
	However, Article 50 of the PIPL states personal information handlers shall establish convenient mechanisms to accept and handle applications from individuals to exercise their rights. Where they reject individuals' requests to exercise their rights, they shall explain the reason.
Controller to controller	
Article 20(2): In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.	See Article 45(2) above.
Technically Feasible	
See Article 20(2) above.	The PIPL does not address technical feasibility.
Exceptions	
See Article 12(5) in section 6.1. above.	The PIPL does not explicitly provide any exceptions to the right to data portability.

⚠ 6. Enforcement



6.1. Monetary penalties

Both the GDPR and the PIPL provide for monetary penalties and set out maximum fines that may be a percentage of an organisation's annual turnover. In addition, neither pieces of legislation provide for imprisonment as a sanction, nor do they impose liability on a DPO. Notably, the PIPL does provide for personal liability including liability on directors and senior management, whereas the GDPR does not.

GDPR	PIPL
Provides for monetary penalties	
The GDPR provides for monetary penalties.	The PIPL provides for monetary penalties.
Issued by	
Article 58(2) Each supervisory authority shall have all of the following corrective powers: [...] (i): to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case.	Article 66: Where personal information is handled in violation of the PIPL or personal information is handled without fulfilling personal information protection duties in accordance with the provisions of the PIPL, the departments responsible for the protection of personal information [...] where correction is refused, a fine [...] [NB: Article 63 of the PIPL outlines the measures that may be adopted by departments responsible for the protection of personal information (see section 6.2. below for further information).]
Fine maximum	
Article 83(5): infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: • the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; • the data subjects' rights pursuant to Articles 12 to 22; • the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; • any obligations pursuant to Member State law adopted under Chapter IX;	Article 66: Where the circumstances of the unlawful acts mentioned in Paragraph 1 of Article of the PIPL are serious, the provincial- or higher-level departments responsible for the protection of personal information shall impose a fine of not more than RMB 50 million (approx. €6.5 million) or not more than 5% of annual revenue [...]

GDPR	PIPL

Fine maxiumum (cont'd)

GDPR	PIPL
• non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1). (6) Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.	

Percentage of turnover

GDPR	PIPL
Under Article 83(4), (5), and (6), fines may be issued that equate to 2% or 4% of the total worldwide annual turnover of the preceding financial year.	See Article 66 above.

Mitigating factors

GDPR	PIPL
Article 83(2): When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: • the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; • the intentional or negligent character of the infringement; • any action taken by the controller or processor to mitigate the damage suffered by data subjects; • the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; • any relevant previous infringements by the controller or processor; • the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; • the categories of personal data affected by the infringement;	The PIPL does not expressly provide mitigating factors.

GDPR	PIPL

Mitigating factors (cont'd)

GDPR	PIPL
• the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; • 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 pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and • any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.	

Imprisonment

GDPR	PIPL
Not applicable.	The PIPL does not explicitly provide for imprisonment. However, Article 71 of the PIPL states that where a violation of the provisions of the PIPL constitutes a violation of public security management, public security management punishment shall be imposed according to the law; where it constitutes a crime, criminal liability is to be investigated according to the law.

DPO liability

GDPR	PIPL
Not applicable.	Not applicable.

6.2. Supervisory authority

Consistent

The GDPR and the PIPL provide for the establishment of a supervisory authority. Similar to the national data protection authorities under the GDPR, enforcement is carried out by individual departments at local level and by the CAC on a national level, with the CAC in particular having special rule making powers under Article 62 of the PIPL. In addition, both the GDPR and PIPL outlined the role and powers of the supervisory authority and require the issuing of annual reports by the same.

GDPR	PIPL
Provides for data protection authority	
Article 51(1): Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').	Article 60: The CAC is responsible for comprehensive planning and coordination of personal information protection work and related supervision and management work. Relevant State Council departments are responsible for personal information protection, supervision, and management work within their respective scope of duties and responsibilities, according to the provisions of the PIPL and relevant laws and administrative regulations. County-level and higher People's governments' relevant departments' personal information protection, supervision, and management duties and responsibilities are determined according to relevant State provisions.
Article 58(1): Each supervisory authority shall have all of the following investigative powers: • to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks; • to carry out investigations in the form of data protection audits; • to carry out a review on certifications issued pursuant to Article 42(7); • to notify the controller or the processor of an alleged infringement of this Regulation; • to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks; • to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.	Article 63: When departments responsible for the protection of personal information perform fulfil personal information protection duties and responsibilities, they may adopt the following measures: • interviewing relevant concerned parties, and investigating circumstances related to personal information handling activities; • consulting and reproducing a concerned party's contracts, records, and receipts as well as other relevant material related to personal information handling activities; • conducting on-site inspections, and conducting investigations of suspected unlawful personal information handling activities; and • inspecting equipment and articles relevant to personal information handling activities; and when there is evidence the equipment or articles are used to engage in illegal personal information handling activities, after reporting to the the principal person-in-charge of the department in writing and receiving approval, they may seal or confiscate them.

GDPR	PIPL
Corrective powers	
Article 58(2): Each supervisory authority shall have all of the following corrective powers: • to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation; • to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation; • to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation; • to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period; • to order the controller to communicate a personal data breach to the data subject; • to impose a temporary or definitive limitation including a ban on processing; • to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to Article 17(2) and Article 19; • to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met; • to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case; • to order the suspension of data flows to a recipient in a third country or to an international organisation.	Article 64: Where departments fulfilling personal information protection duties and responsibilities discover relatively large risks exist in personal information handling activities or personal information security incidents occur, they may conduct a talk with the personal information handler's legal representative or main person responsible according to regulatory powers and procedures, or require personal information handlers to entrust specialised institutions to conduct compliance audits of their personal information handling activities. Personal information handlers shall adopt measures according to requirements to correct the matter and eliminate the vulnerability. Article 66: [...] The departments responsible for the protection of personal information are to order correction, confiscate unlawful income, and order the provisional suspension or termination of service provision of the application programs unlawfully handling personal information.
Authorisation/advisory powers	
Article 58(3): Each supervisory authority shall have all of the following authorisation and advisory powers: • to advise the controller in accordance with the prior consultation procedure referred to in Article 36;	Article 61: Departments responsible for the protection of personal information shall fulfil the following personal information protection duties and responsibilities: • conducting personal information protection propaganda

Authorisation/advisory powers (cont'd)

- to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
- to authorise processing referred to in Article 36(5), if the law of the Member State requires such prior authorisation;
- to issue an opinion and approve draft codes of conduct pursuant to Article 40(5);
- to accredit certification bodies pursuant to Article 43;
- to issue certifications and approve criteria of certification in accordance with Article 42(5);
- to adopt standard data protection clauses referred to in Article 28(8) and in point (d) of Article 46(2);
- to authorise contractual clauses referred to in point (a) of Article 46(3);
- to authorise administrative arrangements referred to in point (b) of Article 46(3);
- to approve binding corporate rules pursuant to Article 47.

and education, and guiding and supervising personal information handlers' conduct of personal information protection work;

- accepting and handling personal information protection-related complaints and reports;
- organising evaluation of the personal information protection situation such as procedures used, and publishing the evaluation results;
- investigating and dealing with unlawful personal information handling activities; and
- other duties and responsibilities provided in laws or administrative regulations.

Tasks of authority

Article 57(1): Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

- monitor and enforce the application of this Regulation;
- promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention;
- advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
- promote the awareness of controllers and processors of their obligations under this Regulation;
- upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, cooperate with the supervisory authorities in other Member States to that end;
- handle complaints lodged by a data subject, or by a

Article 60: The CAC is responsible for comprehensive planning and coordination of personal information protection work and related supervision and management work. Relevant State Council departments are responsible for personal information protection, supervision, and management work within their respective scope of duties and responsibilities, according to the provisions of this Law and relevant laws and administrative regulations.

Article 62: The CAC coordinates overall the following personal information protection work by the relevant departments:

- formulate concrete personal information protection rules and standards;
- formulate specialised personal information protection rules and standards for small-scale personal information handlers and new technologies and new applications for handling sensitive personal information, facial recognition, artificial intelligence, etc.;
- support the research, development, and broad

Tasks of authority (cont'd)

body, organisation or association in accordance with Article 80, and investigate, to the extent appropriate, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;

- cooperate with, including sharing information and provide mutual assistance to, other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation;
- conduct investigations on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
- monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
- adopt standard contractual clauses referred to in Article 28(8) and in point (d) of Article 46(2);
- establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to Article 35(4);
- give advice on the processing operations referred to in Article 36(2);
- encourage the drawing up of codes of conduct pursuant to Article 40(1) and provide an opinion and approve such codes of conduct which provide sufficient safeguards, pursuant to Article 40(5);
- encourage the establishment of data protection certification mechanisms and of data protection seals and marks pursuant to Article 42(1), and approve the criteria of certification pursuant to Article 42(5);
- where applicable, carry out a periodic review of certifications issued in accordance with Article 42(7);
- draft and publish the criteria for accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
- conduct the accreditation of a body for monitoring codes of conduct pursuant to Article 41 and of a certification body pursuant to Article 43;
- authorise contractual clauses and provisions referred to in Article 46(3);

adoption of secure and convenient electronic identity authentication technology, and promote the construction of public online identity authentication services;

- advance the construction of service systems to socialise personal information protection, and support relevant organisations to launch personal information protection evaluation and certification services; and
- perfect personal information protection complaint and reporting work mechanisms.

GDPR	PIPL
Tasks of authority (cont'd)	
approve binding corporate rules pursuant to Article 47; • contribute to the activities of the Board; • keep internal records of infringements of this Regulation and of measures taken in accordance with Article 58(2); and • fulfil any other tasks related to the protection of personal data.	
Annual report	
Article 59: Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board.	Article 65: Departments fulfilling personal information protection duties and responsibilities shall publish contact methods to accept complaints and reports

6.3. Other remedies

Fairly inonsistent

The GDPR and the PIPL provide that data subjects/individuals may seek compensation for damage and harm, respectively. However, the GDPR explicitly clarifies data processor liabilities and the mandating of representatives, while the PIPL is silent on these matters.

GDPR	PIPL
Provides for claims/cause of action	
Article 79: Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.	Article 50: Where a personal information handler rejects an individual's request to exercise their rights, the individual may file a lawsuit with a People's Court according to the law. Article 70: Where personal information handlers handle personal information in violation of the provisions of the PIPL, infringing on the rights and benefits of many individuals, the People's Procuratorates, statutorily designated consumer organisations, and organisations designated by the CAC may file a lawsuit with a People's Court according to the law.
Material and non-material damage	
Article 82(1): Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.	Article 69 of the PIPL states that where the handling of personal information infringes upon personal information rights and interests and results in harm, and personal information handlers cannot prove they are not at fault, they shall bear compensation and other take responsibility for the infringement. In Article 69 of the PIPL, the responsibility to compensate for infringement shall be determined according to the resulting loss to the individual or the personal information handler's resulting benefits. Where the loss to the individual and the personal information handler's benefits are difficult to determine, determine compensation according to practical conditions.
Mandate for representation	
Article 80(1): The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on	The PIPL does not refer to a mandate for representation. However, Article 70 states that where personal information handlers handle personal information in violation of the provisions of the PIPL, infringing on the rights and benefits of many individuals, the People's Procuratorates, statutorily designated consumer organisations, and

GDPR	PIPL
Mandate for representation (cont'd)	
his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.	organisations designated by the CAC may file a lawsuit with a People's Court according to the law.
Specifies amount for damages	
Not applicable.	The PIPL does not explicitly provide amount for damages.
Processor liability	
Article 82(2): Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.	The PIPL does not explicitly address the liability of entrusted persons. However, Article 59 states: Entrusted persons shall, in accordance with the provisions of the PIPL and the relevant laws and administrative regulations, take the necessary measures to safeguard the security of the personal information processed and assist the personal information processor in fulfilling its obligations under the PIPL.
Exceptions	
Article 82(3): A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.	The PIPL does not address exemption from liability of the abovementioned sections.