



GDPR VS THE WORLD

PART 1 GDPR VS ASIA



China 

Hong Kong

India

Indonesia

Japan

Malaysia

Singapore

South Korea

Thailand

UAE

How much has the GDPR driven data protection worldwide ?

An in-depth comparison of different legislations
around the world based on 35 criteria

Authors



Stéphanie Exposito-Rosso
IT Legal Expert and Main Author



Sumedha Ganjoo
Legal Research Lead



Katia Bouslimani
Chief Legal Research Officer



Adam Ali-Bey
IT Legal Expert



Antoine Piquet
IT Legal Expert



Eloïse Quinzin
IT Legal Expert

We would like to thank Bianca Kunrath, Era Selmani and Ylli Kodza for their feedback. Copy editing, report design, and support for content strategy was provided by platformable.com

The information provided in this publication is general and may not apply in a specific situation. The publishers and authors accept no responsibility for any acts, errors or omissions contained herein. The information provided was verified between October 2021 and August 2022. Note that the regulation is meant to evolve.

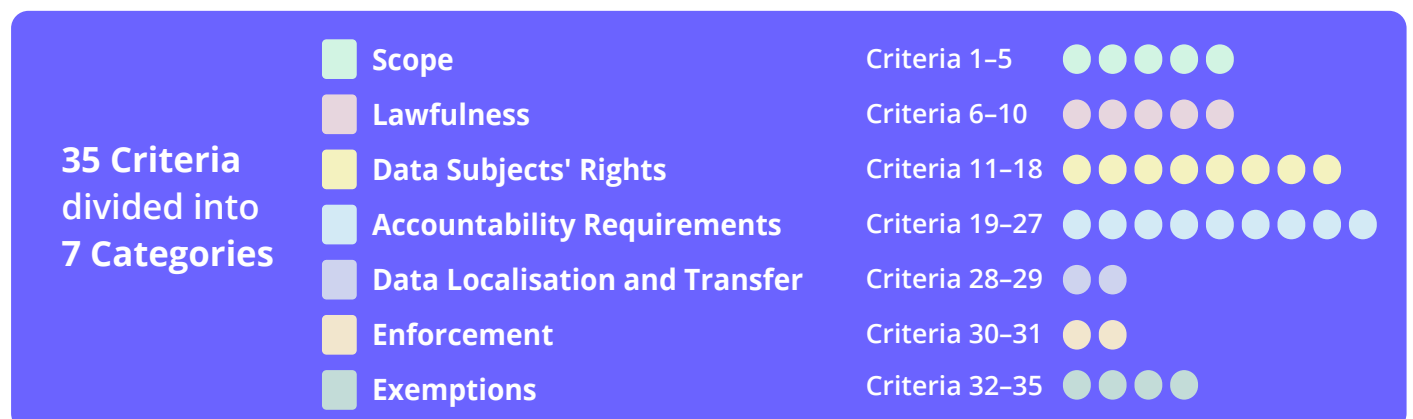
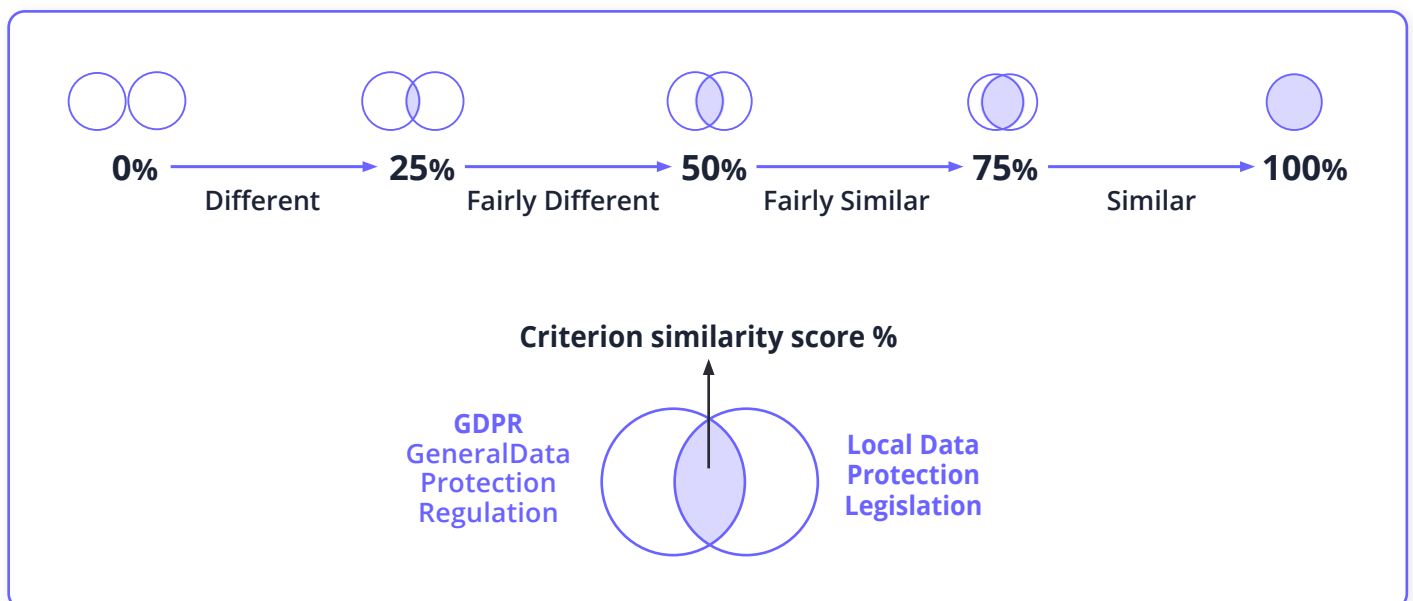
Published September 2022

Welcome to the "GDPR VS" Series

The General Data Protection Regulation (GDPR) was adopted in 2016 by the European Parliament and the European Council, and entered into force on 25 May 2018. Innovative by its extensive scope, provisions and enforcement potential, the GDPR made a lot of noise and required companies to provide efforts of compliance.

25 May 2022 is the fourth anniversary of the GDPR, and a pertinent time to ask: Has the GDPR created "a recipe for the world?" [Code is Law \(Alias.dev\)](#) aims to assess the level of influence of the GDPR in different regions of the world that have adopted or have not adopted new data protection regulations since 2016. The objective is to help companies conduct their gap analysis between different data protection legislations in their data protection compliance efforts.

[Alias.dev](#) chose 35 criteria to compare the GDPR with other data protection legislation, and analysed these criteria through more than 200 sub-criteria. Each criterion is given a similarity score. The score indicates how much effort GDPR-compliant companies will have to engage to comply with data protection legislation outside the EU and understand the data protection culture of the jurisdiction. The similarity score is as follows:



Content

05 List of Acronyms

06 Introduction

07 Scope

Criterion 1. The Territorial Scope /7

Criterion 2. The Subject Matter Scope /8

Criterion 3. Definition of Personal Data /9

Criterion 4. Definition of Sensitive Personal Data /10

Criterion 5. Relevant Parties /11

13 Lawfulness

Criterion 6. Legal Bases /13

Criterion 7. Consent /14

Criterion 8. Legitimate Interest /15

Criterion 9. Conditions for Processing of Sensitive Data /15

Criterion 10. Children /17

18 Data Subjects' Rights

Criterion 11. Transparency Requirements /18

Criterion 12. Right of Access /19

Criterion 13. Right to Data Portability /20

Criterion 14. Right to Rectification /21

Criterion 15. Right to be Forgotten / Right to Erasure /22

Criterion 16. Right to Object /23

Criterion 17. Rights Related to Profiling /23

Criterion 18. Right to Restrict the Use of the Personal Data /24

25 Accountability Requirements

Criterion 19. Appointment of a Representative /25

Criterion 20. Appointment of a DPO /26

Criterion 21. Record of Processing /28

Criterion 22. Data Protection Impact Assessment (DPIA) /29

Criterion 23. Privacy by Design / Right to Erasure /31

Criterion 24. Audit Requirements /31

Criterion 25. Appointment of Processors /32

Criterion 26. Information Security /33

Criterion 27. Breach Notification /35

36 Data Localisation and Transfer

Criterion 28. Data Localisation Requirements /36

Criterion 29. International Data Transfer /37

39 Enforcement

Criterion 30. Data Protection Authority /39

Criterion 31. Penalties /41

43 Exemptions

Criterion 32. Anonymised Data /43

Criterion 33. Social Media Intermediaries and Identity Managements /44

Criterion 34. Exemptions for Research /45

Criterion 35. Application to Public Authorities /45

46 Conclusion

47 Compliance-as-Code: Our Solution

List of Acronyms

C

CAC: Cyberspace Administration of China

D

DPO: Data Protection Officer

DPIA: Data Protection Impact Assessment

G

GDPR: General Data Protection Regulation

P

PIPL: Personal Information Protection Law

Introduction

The Cyberspace Administration of China (CAC) submitted its proposed Regulations on Network Data Security Management (the "Draft Regulations") for public comment on 14 November 2021. The Draft Regulations are intended to implement portions of three existing laws – the Cybersecurity Law (CSL), the Data Security Law (DSL), and the Personal Information Protection Law (PIPL) (collectively, the "Three Laws"). In addition, the Draft Regulations include additional data processing-related obligations. When fully implemented, these regulations would impose even more stringent compliance requirements on businesses than the GDPR.

In China, privacy has a distinct meaning. Individuals, as well as national security, are protected by the legislation. It is one of the strongest data privacy regulations in the world. It is based on Europe's comprehensive General Data Protection Regulation (GDPR), but there are some key differences between the PIPL and the GDPR and other privacy laws throughout the globe. These fundamental distinctions are inspected here in an in-depth study conducted by our research team.

The GDPR was compared with the PIPL based on 35 criteria, including territorial scope, subject matter scope, the definition of personal and sensitive personal data, consent, legitimate interest, localisation of data, data subject's rights, and application to public authorities.

While the PIPL seems very similar to the GDPR, it has certain substantive provisions which are absent in the GDPR. Additionally, some provisions of the GDPR are not part of the PIPL. A high-level analysis of significant matters where the PIPL converges or diverges from the GDPR is provided in this report.

Contrary to the GDPR, there is no specific data protection authority or agency responsible for supervising compliance with personal data laws in China. Under the PIPL, the regulators in charge of the protection of personal data include the Cyberspace Administration of China (CAC), relevant State Council departments, and relevant departments of local governments at the county level and higher. The public security authority, an equivalent to the police, is in charge of practical enforcement, administrative penalties, and crimes related to the infringement of privacy.

Moreover, government authorities supervising specific sectors have various responsibilities when it comes to the supervision of compliance related to data protection. It is the case for the China Banking and Insurance Regulatory Commission (CBIRC), the National Health and Family Planning Commission (NHFPC), the National Medical Products Administration (NMPA), the [Ministry of Science and Technology](#) (MOST), the State Administration for Market Regulation (SAMR), the Ministry of Industry and Information Technology (MIIT), and the Ministry of Transportation (MOT).

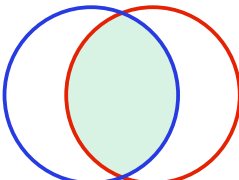
In the PIPL, some notions have different names from the GDPR's:

- The Data Controller is referred to as a Personal Information Handler.
- The Data Processor is referred to as an Entrusted Person.
- The Data Subject is referred to as the Individual.

There are also open definitions in the PIPL where lists end with etc. denoting that additional definitions can be decided on an *ad hoc* basis.


Scope

Criterion 1.
The Territorial Scope



65%

Fairly Similar


GDPR

Article 3

The GDPR is applicable when there is the presence of an "establishment" in the EU, which means that the Data Controller or the Data Processor exercises an effective and real activity (even a minimal one) through stable arrangements.

Extraterritorial scope: applies when a Data Controller or a Data Processor that is located outside the EU processes activities that are related to the offering of goods or services (regardless of the existence of a payment) to Data Subjects in the EU or to the monitoring of their behaviour as far as their behaviour takes place within the EU.

Article 3

PIPL

The PIPL applies to any processing of personal information that happens in China.

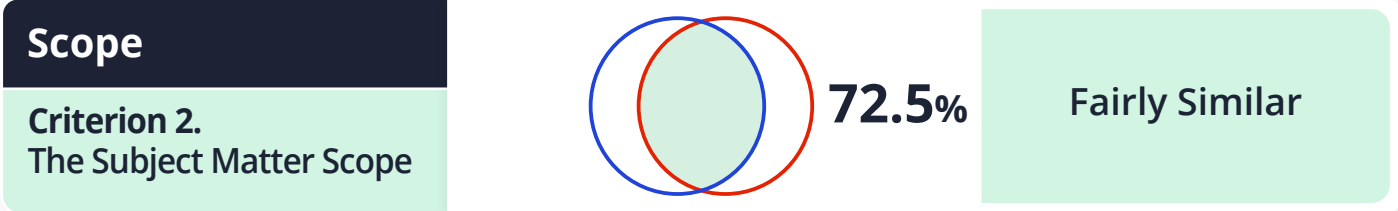
In addition, it also applies to processing activities outside of China that relate to personal information of Individuals in China if the purpose of the processing is:

- The offer of goods or services to Individuals in China.
- The monitoring and evaluation of the activities of Individuals in China.

The PIPL can also apply to processing activities outside of China according to other laws or administrative regulations.

Similar to the GDPR, the PIPL applies to activities related to the processing of personal data of natural persons within the borders of the country. However, contrary to the GDPR, the PIPL applies whether or not the Data Controller (Personal Information Handler in the PIPL) has an establishment in China.

Both the GDPR and PIPL apply outside their territories when the purpose of processing is the offer of goods or services to Individuals residing in the territory. Both laws apply extraterritorially when the Data Controller is monitoring Data Subjects (Individuals in the PIPL) but the scope is slightly different for the GDPR as it applies when the Data Controller monitors Data Subjects' behaviour, and the PIPL applies when the Data Controller monitors and evaluates a Data Subject's activities.



<div>GDPR</div> <div>Article 1</div>	<div>Articles 1, 2, 4, 72</div> <div><div>PIPL</div></div>
<p>The GDPR's aims are clearly defined: to protect the fundamental rights and freedoms of natural persons, in particular their right to the protection of personal data and to protect and encourage the free movement of personal data within the EU.</p> <p>If the data is part of a file system, the GDPR applies to the processing of personal data by automated or non-automated methods.</p> <p>The GDPR does not apply to anonymised data.</p> <p>The GDPR exempts:</p> <ul style="list-style-type: none">• Personal data processed by people for solely personal or domestic reasons that has "no relation to a professional or commercial activity".• Data processed in the context of law enforcement or national security. <p>The GDPR establishes standards for some types of processing, such as processing for journalistic purposes and processing for academic, artistic, or literary expression.</p>	<p>The PIPL aims to protect personal information rights and interests, standardise personal information handling activities, and promote the rational use of personal information. It explicitly provides that no organisation may infringe upon a natural person's personal information rights and interests.</p> <p>The PIPL governs how personal information is "handled". Handling refers to the collection, storage, use, processing, transmission, provision, disclosure, deletion, etc. of personal information. The PIPL does not apply to anonymised data.</p> <p>The PIPL exempts:</p> <ul style="list-style-type: none">• Handling of personal information for personal or family affairs. <p>Where the law contains provisions on personal information handling by the people's governments at all levels and their relevant departments and organisations implementing statistical and archival management activities, those provisions apply.</p>

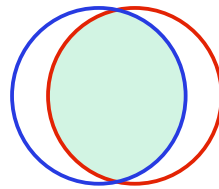
In both cases, the objective of the law is to protect personal information rights and interests. However, the PIPL specifies that it is also meant to "standardise personal information handling activities, and promote the rational use of personal information". The GDPR rather mentions the "fundamental rights and freedom" of natural persons, and the concept of free movement of personal data.

The material scope seems similar, as the notions of "processing" and "handling" on the one hand, and "personal data" and "personal information" on the other hand, have the same scope. Contrary to the GDPR, the PIPL does not require personal information to be part of a file system to be subject to protection. Both laws exclude anonymised data from their scope.

Both laws exempt the processing of personal data for personal reasons ("solely personal or domestic reasons" in the GDPR; "for personal or family affairs" in the PIPL). The GDPR excludes law enforcement or national security processing from its scope, and provides special standards for some types of processing. The PIPL excludes its applicability to processing that is already subject to other laws (handling by the people's governments, statistical and archival management activities).

Scope

Criterion 3. Definition of Personal Data



80%

Similar



GDPR

Article 4, (1), (13), (14), (15),
Article 9

Personal data is defined by the GDPR as:

- Any information relating to an identified or identifiable natural person ("Data Subject").

An identifiable natural person, according to the GDPR, 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 one or more factors specific to that natural person's physical, physiological, genetic, mental, economic, cultural, or social identity.

Online identifiers, such as IP addresses, cookie identifiers, and radio frequency identifying tags, are considered personal data under the GDPR.

The GDPR does not apply to deceased people.

The GDPR does not apply to data that has been "anonymised" that can no longer be used to identify the Data Subject.

Article 4



PIPL

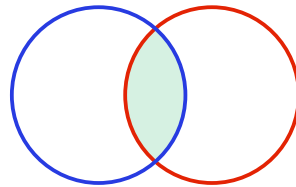
Personal information is all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymisation handling.

In both instances, the term "data" refers to "all types of information". The PIPL does clarify how this information is to be supported, stating that it may be "recorded electronically or by other ways". However, there is no indication of the kind of identification that may be used to assist in identifying a person. Similar to the GDPR, the PIPL's definition of personal information specifies that information must be "related to identified or identifiable natural people" in order for the law to apply.

In both instances, anonymised data is excluded from the scope of the law's applicability.

Scope

Criterion 4. Definition of Sensitive Personal Data



37%

Fairly Different



GDPR

Article 9

The GDPR's definition of sensitive personal data covers:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- The processing of genetic data and biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

Article 28

PIPL



Sensitive personal information refers to personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons or grave harm to personal or property security.

- The definition includes information on:
 - Biometric characteristics
 - Religious beliefs
 - Specially-designated status
 - Medical health
 - Financial accounts
 - Individual location tracking
 - Personal information of minors under the age of 14
 - Etc.

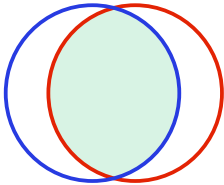
Both the GDPR and the PIPL include biometric data, religious beliefs, and medical health data in the definition of sensitive personal data. However, the GDPR's definition of sensitive personal data is quite different from that of the PIPL.

In the PIPL, the concept of sensitive personal data is interpreted differently than in the GDPR. Indeed, the PIPL considers information to be sensitive if it is leaked or unlawfully exploited in a way that "endangers the dignity of natural persons or the security of property". Moreover, the PIPL classifies "financial accounts, individual location monitoring, specifically designated status, and personal information of children under the age of 14" as sensitive personal information by default. The inclusion of "etc." in the legislation denotes that additional definitions can be decided on an *ad hoc* basis.

Contrary to the GDPR, the PIPL does not explicitly include ethnic origin, political opinions, philosophical beliefs, genetic data, or a natural person's sex life or sexual orientation. Nevertheless, these data could be qualified as sensitive data if the leakage consequences criterion is met.

Scope

Criterion 5.
Relevant Parties



75%

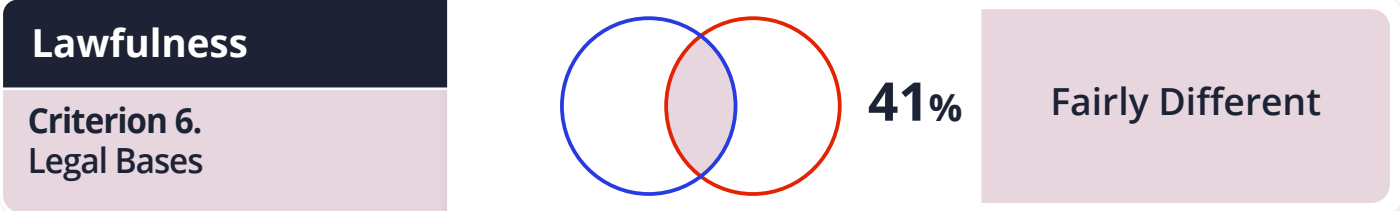
Similar



<div> GDPR</div> <div>Articles 4 (7), 28, 30, 82</div>	<div>Articles 21, 73</div> <div>PIPL </div>
<ul style="list-style-type: none">• A Data Controller is a natural or legal person, public authority agency, or other organisation that, alone or collectively with others, decides the goals and methods of processing personal data.• A Data Processor is a natural or legal person, government agency, or other entity that processes personal data on behalf of the Data Controller. <p>Data Controllers must adhere to the purpose restriction and accuracy principles, and repair any inaccurate or incomplete personal data held by a Data Subject. They are required to put in place technological and organisational security measures, and alert supervisory authorities in the event of a data breach.</p> <p>Data Controllers and Data Processors are required to retain records of processing operations, although small businesses are exempt from this need. Data Controllers and Data Processors can also designate a DPO.</p> <p>Where processing is carried out on behalf of a Data Controller, the Data Controller must only use Data Processors who can provide sufficient guarantees to implement the appropriate technical and organisational measures to ensure that processing complies with the GDPR's requirements and protects the Data Subject's rights. Furthermore, without the Data Controller's previous explicit or general written authorisation, the Data Processor may not engage another Data Processor.</p> <p>No examination system is named. However, the GDPR states that "time limits for erasure or periodic review should be established by the Data Controller".</p> <p>In specific cases, the GDPR requires a Data Controller or Data Processor to complete a DPIA.</p>	<ul style="list-style-type: none">• A Personal Information Handler refers to organisations and Individuals that, in personal information handling activities, autonomously decide handling purposes and handling methods.• Entrusted Persons refers to the person the Personal Information Handler will entrust with the handling of personal information. <p>When entrusting the handling of personal information, the Personal Information Handlers shall conclude an agreement with the Entrusted Person on the purpose for:</p> <ul style="list-style-type: none">• Entrusted handling• The time limit• The handling method• Categories of personal information• Protection measures, as well as the rights and duties of both sides, etc.• Conduct supervision of the personal information handling activities of the Entrusted Person <p>Entrusted Persons shall handle personal information according to the agreement. They may not handle personal information for handling purposes or in handling methods, etc., that are not provided in the agreement. 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.</p> <p>An Entrusted Person may not further entrust personal information handling to other persons without the consent of the Personal Information Handler.</p>

The definition of "Data Controller" and "Personal Information Handler" is quite similar as they refer to the person who decides the means and goals of the processing. The notions of "Data Processor" and "Entrusted Person" also seem to have similar meanings.

Both laws require the Data Controller (Personal Information Handler in the PIPL) and the Data Processor (Entrusted Person in the PIPL) to conclude a contract setting out the characteristics of the processing. The PIPL seems to require more details than the GDPR as it requires the Personal Information Handler to specify the handling methods and the protection measures.

Both laws require the Data Controller to monitor the Data Processor's ability to ensure the security of personal data. However, the PIPL is more restrictive as it requires the Data Controller to conduct supervision of the personal information handling activities of the Data Processor.



<div> GDPR</div> <div>Articles 6-10 Recitals 39-48</div>	<div>Article 13</div> <div>PIPL </div>
<p>Processing is lawful only if and to the extent that at least one of the following applies:</p> <ul style="list-style-type: none">• The Data Subject has given consent to the processing of their 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 Data 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 Data Controller.• Processing is necessary for the purposes of the legitimate interests pursued by the Data 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.	<p>Personal Information Handlers may only handle personal information where they conform to one of the following circumstances:</p> <ul style="list-style-type: none">• 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 according to lawfully formulated labour rules and structures and lawfully concluded collective 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.• Other circumstances provided in laws and administrative regulations. <p>In the PIPL, consent is the legal basis by default for the processing of personal data.</p>

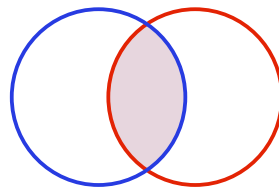
Both laws define consent as a legal basis, but contrary to the GDPR, the PIPL seems to require the consent of the Data Subject (Individual in the PIPL) as a default legal basis, the other legal bases being derogations of the obtention of consent.

Some legal bases are similar in the GDPR and the PIPL: the consent of the Data Subject, the fulfilment of a contract, the compliance with legal obligations, the protection of vital interests, and the performance of tasks carried out in the public interest. However, there are substantial differences.

Contrary to the GDPR, the PIPL does not provide a legal basis for legitimate interests. However, the PIPL provides additional legal bases that are not provided in the GDPR, such as human resources management, sudden public health incidents, the security of a person's property under emergency conditions, the implementation of news reporting, and public opinion supervision and the handling of data disclosed by persons themselves or otherwise already lawfully disclosed.

Lawfulness

Criterion 7. Consent



45%

Fairly Different



Articles 4(11), 7, Recitals 32, 42, 43

The GDPR establishes a set of criteria for gaining valid consent:

- Consent must be freely given, specific and informed.
- It must be granted by an unambiguous, affirmative action where the Data Subject signifies agreement to the processing of personal data relating to them.
- Generally, provision of a service cannot be made conditional on obtaining consent for processing that is not necessary for the service.
- A request for consent must be distinct from any other terms and conditions.
- The consent can be easily withdrawn at any moment "without prejudice".

Articles 14-15

PIPL



The consent of the Individual must be given under the precondition of full knowledge in a voluntary and explicit statement. Some additional laws or administrative regulations can also provide that the consent shall be specific or written.

Any change occurring in the purpose or the method of personal information handling or in the categories of handled personal information requires the Personal Information Handler to obtain a new consent from the Individual.

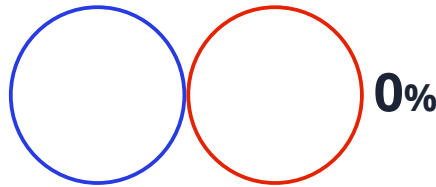
The PIPL requires Personal Information Handlers provide Individuals with a convenient way to withdraw their consent.

Both the GDPR and the PIPL require the consent to be informed. According to the GDPR, consent should also be freely given, which means in particular that consent cannot be a condition for the provision of a service, that the request for consent must be distinct from any other terms and conditions and that the Data Subject is given the right to withdraw their consent at any time. On the other hand, the PIPL requires the consent to be "voluntary", which is a close notion to "freely given", as it also grants the Individual the right to withdraw their consent. However, voluntary consent is more permissive than the GDPR's freely given consent.

The PIPL requires consent to be explicit, while the GDPR only requires explicit consent for special legal bases such as third-country transfers. The PIPL only requires specific consent when a specific law provision requires it, while it is a general requirement in the GDPR. Finally, the PIPL can require written consent when specific provisions require it.

Lawfulness

Criterion 8. Legitimate Interest



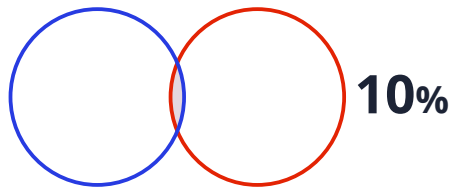
0%

Different

Contrary to the GDPR, the PIPL does not provide a legitimate interest legal basis.

Lawfulness

Criterion 9. Conditions for the Processing of Sensitive Data



10%

Different

1 2



GDPR

Articles 9, 10, Recital 47

There are ten legal bases for processing sensitive data, subject to further additions by Member States:

1. Explicit consent.
2. To comply with obligations and exercising rights in the context of employment and social security.
3. Life protection and vital interests.
4. Legitimate activities (by a foundation, association or other non-profit body with a political, philosophical, religious, or trade union aim, which processes data about its members).
5. Establishment, exercise, or defence in legal claims.
6. Data manifestly made public by the individual.
7. Substantial public interest defined by law.
8. Preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment.
9. Substantial public interest in health.
10. Archiving, scientific, or historical research purposes.

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is

Articles 29-32

PIPL



The Individual's separate consent must be obtained when handling sensitive personal information. Moreover, in some cases, laws or administrative regulations provide that written consent must be obtained.

Besides the separate consent when handling sensitive personal information, Personal Information Handlers must also notify Individuals about the necessity and influence on the Individual's rights and interests in handling the sensitive personal information, except where the PIPL provides that it is permitted not to notify the Individuals.

The consent of the parent or other guardian is mandatory when handling the personal information of minors under 14. In that case, the Personal Information Handlers must formulate specialised personal information handling rules.

Where laws or administrative regulations provide that relevant administrative licences must be obtained or other restrictions apply to the handling of sensitive personal information, those provisions are to be followed.

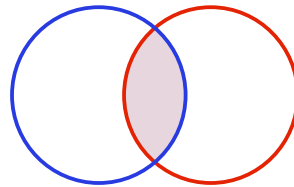
authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of Data Subjects. Any comprehensive register of criminal convictions shall be kept only under the control of an official authority.

The conditions for processing sensitive personal data are very different in the GDPR and in the PIPL. In the GDPR, Data Controllers can process sensitive personal data as long as they can justify the processing according to one of the ten legal bases provided by Article 9, including explicit consent. In the PIPL, special categories of personal information can only be handled with the separate consent of the Data Subject (Individual in the PIPL), that is also required to be written in some situations.

Because the PIPL provides that the personal information of minors under 14 years is sensitive data, the PIPL requires the consent of the parent or guardian. The GDPR does not define children's personal data as sensitive data, however, it also requires the consent of the parents when the child is under 16 or sometimes 13 years old, according to national laws (see criterion 10).

Lawfulness

Criterion 10. Children



35%

Fairly Different



Articles 6, 8, 12, 40, 57,
Recitals 38, 58, 75

The GDPR doesn't define the terms "child" or "children". However, children are considered "vulnerable natural people" under the GDPR, who need special protection when it comes to their personal data.

For delivering information society services to a child under the age of 16, the consent of a parent or guardian is necessary if the processing is based on consent. This age restriction may be lowered to 13 by EU member states.

When children's personal data is used for marketing or gathered for information society services presented directly to children, special protection should be provided.

Where any information is intended exclusively for a child, Data Controllers shall take necessary means to convey information relevant to processing in a brief, transparent, comprehensible, and readily available manner, using clear and simple language that the child may easily comprehend.

In the case of information society services, the GDPR's requirements on the appropriate circumstances for processing children's data apply.

Article 31

PIPL



Personal information of minors under 14 is defined as sensitive personal data.

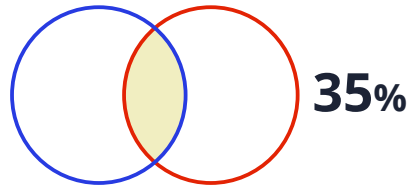
The consent of the parent or other guardian is mandatory when handling the personal information of minors under 14. In that case, the Personal Information Handlers must formulate specialised personal information handling rules.

Both the GDPR and the PIPL require the children's parents or other guardian to consent to process children's data. In the GDPR, the notion of children refers to minors under the age of 16, and EU Member States can lower it to 13. In the PIPL, it refers to minors under 14 years old.

The PIPL protects the data of minors under 14 years old as sensitive data, requiring special protection of this data. On the other hand, the GDPR only protects them in the prism of children's data, and requires Data Controllers to provide information adapted to children.

Data Subjects' Rights

Criterion 11. Transparency Requirements



Fairly Different



Article 12, Recital 58

The GDPR explicitly refers to the principle of transparency, which involves providing information to the Data Subject. The information must be "concise, easily accessible and easy to understand" through the use of "clear and simple language".

The information to be provided is precisely detailed in the GDPR.

Article 7



The principles of openness and transparency shall be observed in the handling of personal information. The rules for handling personal information must be disclosed, clearly indicating the purpose, method, and scope of handling.

The GDPR is more demanding than the PIPL in terms of transparency requirements. In the GDPR, the information to provide to the Data Subject is precisely detailed, and the Data Controller (Personal Information Handler in the PIPL) must provide this information in a way that is concise, easily accessible, and easy to understand, using clear and simple language. In the PIPL, the Data Controller is also required to provide information in a clear way, but the information which must be provided is more limited. There is no provision regarding the accessibility of the information or the language used.

Data Subjects' Rights

Criterion 12.
Right of Access

30%

Fairly Different

<div> GDPR</div> <div>Articles 12, 15, Recitals 59-64</div>	<div>Articles 45, 49, 50 (17§1, 18§1)</div> <div>PIPL </div>
<p>Data Subjects have the right to access the personal data that is processed by a Data Controller.</p> <p>According to the GDPR, the Data Controller must provide the following information when responding to an access request:</p> <ul style="list-style-type: none">• The recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organisations.• 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 rectification from the Data Controller. <p>According to the GDPR, the right of access shall not infringe on others' rights or freedoms, particularly those connected to trade secrets.</p> <p>Requests from Data Subjects under this right must be responded to without "undue delay" and in any case within one month of receipt.</p> <p>The right to access is unrestricted. A charge may be required in certain cases, particularly when the demands are unwarranted, unreasonable, or recurrent.</p> <p>Data Subjects must be able to submit their requests in a number of ways, including verbally and by technological means. In addition, when a request is made using electronic means, the Data Controller shall respond via electronic means as well.</p>	<p>Individuals have the right to consult and copy their personal information from Personal Information Handlers.</p> <p>When an Individual requests to consult or copy their personal information, Personal Information Handlers shall provide it in a timely manner.</p> <p>When a natural person is deceased, their next of kin may, for the sake of their own lawful, legitimate interests, exercise the rights of access to consult, copy, correct, delete, etc., the personal information of the deceased, except when the deceased has arranged otherwise before their death.</p> <p>Personal Information Handlers shall establish convenient mechanisms to accept and handle applications from Individuals to exercise their rights. Where they reject an Individual's request to exercise their rights, they shall explain the reason.</p> <p>Laws or administrative regulations can exempt Personal Information Handlers from providing Individuals with the right to consult and copy their personal information. State Institutions are also exempted from providing Individuals with the right to consult and copy their personal information when it impedes the fulfilment of their statutory duties and responsibilities.</p> <p>Where Personal Information Handlers reject an Individual's request to exercise their rights, Individuals may file a lawsuit with a People's Court according to the law.</p>

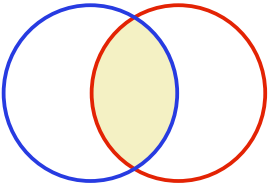
Individuals have the right to consult and copy their personal information from Personal Information Handlers in the PIPL, while the GDPR provides a right to access, including access to the personal data processed and to information about their processing.

In the PIPL, no details are given as to what information is included in the right of access nor under what format or conditions, except concerning the delay, which must be "in a timely manner" in both cases. On the other hand, the GDPR specifies that the right to access is free of charge, the conditions in which it can be denied, and the maximum delay of response.

Contrary to the GDPR, the PIPL clearly establishes a capacity for a deceased person's kin to exercise their right to consult, copy, correct, or delete this person's personal information, except when the deceased has stated otherwise before their death. The conditions of this right being the Data Subject and kin's s lawful, legitimate interests. The GDPR does not recognise such a capacity.


Data Subjects' Rights

Criterion 13.
Right to Data Portability



50%

Fairly Similar

GDPR

Article 20


Data subjects have the right to data portability under the GDPR.

When processing is based on consent, contract, or automatic methods, data subjects have the right to obtain their personal data in a structured, generally used, and machine-readable format.

Where technically practicable, data subjects have the right to send their personal data in the aforementioned form directly to another controller. The GDPR stipulates that the right to data portability shall not jeopardise other people's rights or freedoms.

The GDPR does not make it mandatory for a data controller to keep a record of the reasons for refusing a data portability request.

Articles 45, 50

PIPL

When an Individual requests that their personal information be transferred to a Personal Information Handler that they designate, which meets the conditions of the State Cybersecurity and Informatization Department, Personal Information Handlers shall provide a channel to transfer it.

Moreover, Personal Information Handlers shall establish convenient mechanisms to accept and handle applications from Individuals to exercise their rights. If they reject an Individual's request to exercise their rights, they must explain the reason.

Additionally, if Personal Information Handlers reject an Individual's request to exercise their rights, the Individual may file a lawsuit with a People's Court according to the law.

The right to access and to portability are teamed up together in the PIPL. Similarly to the GDPR, a reasonable delay must be respected and Personal Information Handlers must provide a way to transfer the data.

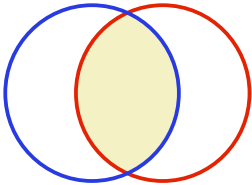
Contrary to the GDPR, the PIPL provides that an Individual has the right to request a Personal Information Handler transfer their personal information to another Personal Information Handler, only when such a transfer satisfies the requirements of the Cybersecurity Administration of China (CAC).

ALIAS Research Report 2022

20


Data Subjects' Rights

Criterion 14.
Right to Rectification



60%

Fairly Similar

GDPR


Article 16

Data Subjects have the right to correct inaccurate personal data and complete incomplete personal data.

Where personal data is updated, it must be communicated to each recipient to which it was disclosed, unless this would involve disproportionate effort.

The Data Controller must restrict processing where the accuracy of the data is disputed for the time needed to verify the request.

Articles 46, 50

PIPL

Where an Individual discovers that their personal information is incorrect or incomplete, they have the right to request Personal Information Handlers correct or complete their personal information.

Where an Individual requests to correct or complete their personal information, Personal Information Handlers shall verify the personal information and correct or complete it in a timely manner.

Personal Information Handlers shall establish convenient mechanisms to accept and handle applications from Individuals to exercise their rights. Where they reject an Individual's request to exercise their rights, they shall explain the reason.

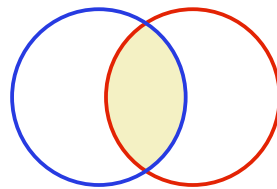
The right to rectification is similar in both the GDPR and PIPL. However, contrary to the GDPR, the PIPL does not provide an obligation to communicate to each recipient to which incomplete or incorrect data was disclosed, nor any limitation of processing.

ALIAS Research Report 2022

21

Data Subjects' Rights

Criterion 15.
Right to be Forgotten /
Right to Erasure



46%

Fairly Different



GDPR

Articles 12, 17 Recitals 59, 65-66

The right to be forgotten applies to specific circumstances, such as when a Data Subject's consent is revoked and there is no other legal basis for processing, or when personal data is no longer required for the purposes for which it was obtained.

The right to erasure/to be forgotten is unrestricted. However, there are certain circumstances in which a charge may be demanded, such as when demands are baseless, unreasonable, or frequent.

If the Data Controller has made personal data public and is required to erase the personal data, the Data Controller shall take reasonable steps, including technical measures, to notify Data Controllers processing the personal data that the Data Subject has requested the erasure by such Data Controllers of any links to, or copy or replication of those personal data, taking into account the available technology and the cost of implementation.

The GDPR sets out exceptions to the right to erasure in the case of:

- Conflict with freedom of speech and information.
- Compliance with public interest objectives in the field of public health.
- Creation, exercise, or defence of legal claims.
- Compliance with legal duties for a public interest purpose.

Under this right, Data Subject requests must be responded to "without excessive delay and in any case within one month of receipt of request".

Article 47

PIPL



Personal Information Handlers shall proactively delete personal information where one of the following circumstances occurs:

- 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.
- Other circumstances provided by laws or administrative regulations.

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.

Personal Information Handlers shall establish convenient mechanisms to accept and handle applications from Individuals to exercise their rights. Where they reject an Individual's request to exercise their rights, they shall explain the reason. In such a case, an Individual may file a lawsuit with a People's Court according to the law.

The scope of the right to erasure is broader in the PIPL, in particular, because the PIPL provides that laws or administrative regulations can establish additional grounds for the right to erasure.

Contrary to the GDPR, the PIPL does not set out any exceptions to the right of erasure. Moreover, it provides for the discontinuation of the personal information handling, except for storage and necessary security protection measures "where the retention period provided by laws or administrative regulations has not expired, or personal information deletion is technically hard to realise". The GDPR does not provide for such a situation.

Data Subjects' Rights

Criterion 16.
Right to Object

0%

Different

Contrary to the GDPR, the PIPL does not provide a right to object.

Data Subjects' Rights

Criterion 17.
Rights Related to Profiling

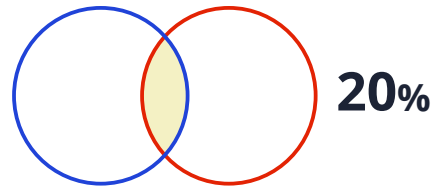
0%

Different

Rights related to profiling are explicitly contained in the GDPR. Such rights do not seem to contain an equivalent in the PIPL.

Data Subjects' Rights

Criterion 18.
Right to Restrict the Use of
the Personal Data



Different



Article 18

The Data Subject shall have the right to obtain from the Data Controller restriction of processing if:

- The accuracy of the personal data is contested by the Data Subject, for a period enabling the Data 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.
- The Data 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 pending the verification of whether the legitimate grounds of the Data Controller override those of the Data Subject.

Article 47

PIPL



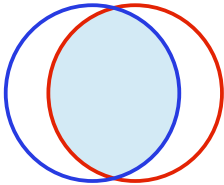
The PIPL only provides the restriction over the use of personal information in the context of the right of erasure.

When a Personal Information Handler cannot erase the data because the retention period provided by laws or administrative regulation has not expired or because the personal information deletion is technically hard to realise, the Personal Information Handler shall cease personal information handling except for storage and taking necessary security protective measures.

Both the GDPR and PIPL require the Data Controller (Personal Information Handler in the PIPL) to restrict the use of the personal data in some circumstances. However, the scope is very different. The PIPL provides a very limited scope related to the inability of the Personal Information Handler to erase personal information at the request of the Individual because of legal or technical reasons. The GDPR provides more grounds to the right to restrict the use of personal data, including the verification induced by the exercise of rights by the Data Subject, the necessity for legal claims, and the request of the Data Subject.



Accountability Requirements

Criterion 19. Appointment of a Representative



75%

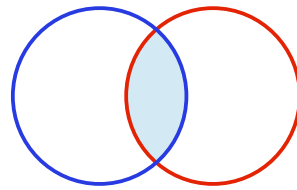
Similar

<div> GDPR</div> <div>Article 27, Recital 80</div>	<div>Article 53</div> <div>PIPL </div>
<p>Data Controllers and Data Processors not established in the EU (but that are subject to the GDPR) must appoint a representative in the EU, except if processing is occasional and does not involve large-scale processing of sensitive data.</p>	<p>Personal Information Handlers outside the borders of the People's Republic of China, shall establish a dedicated entity or appoint a representative within the borders of the People's Republic of China to be responsible for matters related to the personal information they handle.</p> <p>They are to report the name of the relevant entity or the personal name of the representative and contact method, etc., to the departments fulfilling personal information protection duties and responsibilities.</p>

Contrary to the GDPR, the PIPL states that the Personal Information Handlers must report the name and contact method to the departments fulfilling personal information protection duties and responsibilities. In the GDPR, there is no such obligation.

Accountability Requirements

Criterion 20. Appointment of a DPO



37.5%

Fairly Different



Designation

Data Controllers and Data Processors, as well as their representatives, are obliged to designate a DPO under the GDPR, in any case where:

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity.
- The core activities of a Data Controller or Data Processor consist of processing operations that, by their nature, scope, and/or purposes, require regular and systematic monitoring of Data Subjects on a large scale.
- The core activities of the consortia consist of processing on a large scale sensitive data or personal data relating to criminal convictions and offences.

A group may nominate a single DPO who must be reachable by all establishments. When a public authority or body is the Data Controller or Data Processor, a single DPO might be appointed for many public authorities or bodies, depending on their organisational structure and size.

The DPO shall be designated on the basis of professional qualities, in particular expert knowledge of data protection law and practises.

Tasks and responsibilities

The DPO have at least the following tasks:

- To inform/advise the Data Controller or Data Processor and monitor compliance with their obligation under GDPR and other EU/national law applying to processing.
- To provide advice and monitor performance of Data Protection Impact Assessments (DPIA).
- To cooperate and act as a contact point with supervisory authorities.

Article 52



Designation

Personal Information Handlers that handle personal information reaching quantities established by the State Cybersecurity and Informatization Department shall appoint Personal Information Protection Officers (PIPO).

The threshold that triggers the obligation to designate a PIPO is unclear as it has not been defined by the CAC yet. In 2020, the Personal Information Security Specification recommended the establishment of a full-time post and department dedicated to personal information security work when:

- The main business activity involves the processing of personal information and employs more than 200 people.
- The business processes or is estimated to process the personal information of more than 1,000,000 Individuals.
- The business processes the sensitive personal information of more than 100,000 Individuals.

Task and responsibilities

The PIPO is responsible for supervising personal information handling activities as well as adopting protection measures, etc.

The PIPO also is a contact point for Individuals and regulators as Personal Information Handlers shall disclose the methods of contacting PIPOs, and report the personal names of the officers and contact methods to the departments fulfilling personal information protection duties and responsibilities.

Position

The DPO must be involved in all issues relating to personal data protection, and must be provided all resources necessary to perform their tasks.

The DPO is independent and shall neither receive any instructions regarding the exercise of their tasks nor be dismissed or penalised for performing these tasks.

The DPO can fulfil other tasks and duties, but the Data Controller/Data Processor must verify that these tasks do not result in a conflict of interest.

The threshold triggering the obligation to designate a DPO or a PIPO differs in the GDPR and the PIPL. The GDPR establishes that public Data Controllers are bound to designate a DPO. Other Data Controllers must designate a DPO when their core activities require a regular and systematic monitoring of Data Subjects on a large scale or when their core activities consist of processing sensitive data or personal data on a large scale.

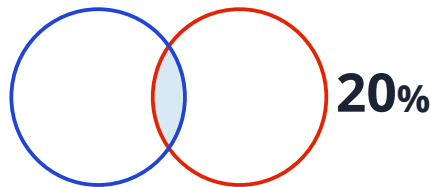
On the other hand, the PIPL's volume of personal information that triggers the threshold is yet to be determined. However, it could be similar to what the Personal Information Security Specification recommended. In this case, the PIPL would also define thresholds according to the nature of personal information: the processing of the personal information of 1,000,000 Individuals and the processing of the sensitive personal information of 100,000 Individuals. The PIPL would also require the designation of a PIPO when the business's core activities are the processing of personal data and the business has more than 200 employees.

Contrary to the PIPL, the GDPR precisely defines the duties and role of the DPO. Under the PIPL, the Personal Information Protection Officers are responsible for supervising personal information handling activities as well as adopting protection measures. Under the GDPR, they have more tasks and responsibilities as they also have to inform, advise the Data Controller or Data Processor, and monitor compliance with their obligation under GDPR and other EU/national law applying to processing. They also have to monitor performance of Data Protection Impact Assessments (DPIA) and cooperate and act as a contact point with the supervisory authority.

There is no further information concerning the necessary qualities and expert knowledge, nor whether they must remain independent and have the needed tools to carry out their responsibilities.

Accountability Requirements

Criterion 21. Record of Processing



Different



GDPR

Article 30, Recital 82

Data Controllers and Data Processors are required to keep a record of processing actions under their control. Furthermore, the GDPR establishes a list of data that a Data Controller must keep track of:

- The Data Controller's name and contact information.
- The purposes of the processing.
- A description of the categories of personal data.
- The categories of recipients to whom the personal data will be disclosed.
- The estimated time for erasure of the categories of data.
- A general description of the technical and organisational security measures used.

The GDPR also establishes a similar list for Data Processors, mandates that records be kept in writing or electronically, and specifies exceptions for businesses with fewer than 250 employees, unless the processing is likely to jeopardise Data Subjects' rights and freedoms, is not routine, or involves special categories of data.

Articles 55, 56

PIPL



The PIPL provides that Personal Information Handlers must keep records of their processing activities in the following scenarios:

- When handling sensitive personal information.
- When making use of personal information in automated decision-making.
- When entrusting the handling of personal information, or otherwise disclosing the same, to other entities.
- When transferring personal information overseas.
- Other handling activities that have a significant impact on the interests of Data Subjects.

The PIPL clarifies that records of processing should be kept for at least three years.

More precision about the records of personal information processing activities could be issued as the Personal Information Security Specification of 2020 already recommended to include:

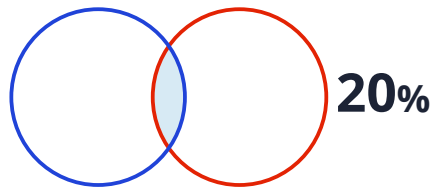
- The type, amount and source of the personal information involved.
- Differentiated processing purposes and scenarios of personal information use based on business functions and consent, as well as information such as entrusted processing, sharing, transfer, public disclosure, and whether cross-border transfer is involved.
- Information systems, organisations, and personnel associated with every step of the personal information processing activity.

The PIPL provides for various conditions under which records of processing must be maintained. The GDPR requires Data Controllers to maintain a record of processing activities unless the business has fewer than 250 employees and when the processing is not likely to jeopardise a Data Subject's rights and freedoms, is routine, or does not involve special categories of data.

Contrary to the PIPL, the GDPR focuses more on functionality aspects as it defines the conditions in which processing records must be maintained, whilst the PIPL gives no information about this topic besides the fact that it must be kept for at least three years. Further specifications for the PIPL may be issued and could follow the Personal Information Security Specification of 2020's recommendations.

Accountability Requirements

Criterion 22. Data Protection Impact Assessment (DPIA)



Different



GDPR

Article 35

The GDPR requires Data Controllers to carry out a DPIA, in particular using new technologies, when the processing is likely to result in a high risk to the rights and freedoms of natural persons.

A DPIA is particularly required in the following situations:

- 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 sensitive data.
- Systematic monitoring of a publicly accessible area on a large scale.

At the very least, the evaluation must include the following:

- A systematic description of the proposed processing operations and lawful processing purposes.
- The need and proportionality of the operations in connection to the purposes.
- Risks to Data Subjects' rights and freedoms.

Article 55

PIPL



When one of the following circumstances is present, Personal Information Handlers shall conduct a Personal Information Protection Impact Assessment (PIPIA) in advance and record the handling situation:

- 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.
- Other personal information handling activities with a major influence on Individuals.

The PIPL does not provide the elements that the evaluation shall include, but the Personal Information Security Specification of 2020 recommended the Personal Information Security Impact Assessment to include:

- Whether the collection of personal information complies with the principles of explicit purposes, independent consent, and minimum necessary.
- Whether the processing of personal information may cause adverse impacts on the lawful rights and interests of Individuals, including whether it could endanger personal or property safety, damage personal reputation or physical and mental health, or lead to differentiated treatment.
- The effectiveness of personal information security measures.
- Risks that the anonymised or de-identified data set, either alone or converged with other data sets, can become identified again.
- Possible adverse impacts of the sharing, transfer, and public disclosure of personal information on the lawful rights and interests of Data Subjects.
- Possible adverse impacts on the lawful rights and interests of Data Subjects in the case of a security incident.

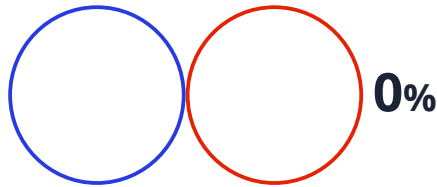
Both the GDPR and PIPL require the Data Controller (Personal Information Handler in the PIPL) to carry out a DPIA (PIPIA in the PIPL) when the processing is estimated to pose specific risks for Data Subjects. However, the assessment of what poses a specific risk differs.

Contrary to the PIPL, the GDPR provides that a DPIA has to be carried out when the processing is likely to result in a high risk to the rights and freedoms of natural persons, in particular when the Data Controller uses technology. This general condition is not present in the PIPL, which defines specific risky situations. However, the PIPL requires a DPIA to be carried out when personal information handling activities have a major influence on the Individuals, which can encompass high risks to rights and freedoms.

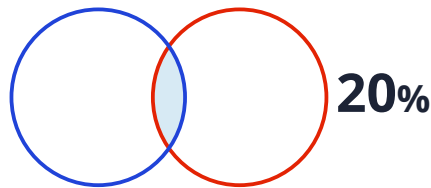
Both the GDPR and the PIPL hold the view that automated decision-making and sensitive personal data processing are high-risk activities that require a DPIA. The PIPL provides a broader obligation than the GDPR as it requires a PIPIA for any processing using personal information in order to conduct automated decision-making and any handling of sensitive personal information. On the other hand, the GDPR only requires the DPIA to be carried out when there is a systematic and extensive evaluation of personal aspects based on automated processing or profiling and when sensitive personal data is processed on a large scale.

Contrary to the GDPR, the PIPL requires a PIPIA when the Personal Information Handler discloses the personal information either to an Entrusted Person, to another Entrusted Person or by any other way. The PIPL also requires a PIPIA to be carried out when the Personal Information Handler provides personal information abroad, whereas the GDPR does not. Contrary to the PIPL, the GDPR requires from the Data Controller a DPIA when the Data Controller systematically monitors a publicly accessible area on a regular basis.

Finally, the PIPL does not give any information about what the evaluation must include, whereas the GDPR is a lot more precise and clear concerning the modalities. However, the Personal Information Security Specification of 2020 recommends including some specific information in the Personal Information Security Impact Assessment.

Accountability Requirements**Criterion 23.**
Privacy by Design**Different**

Contrary to the GDPR, the PIPL does not explicitly provide a privacy by design principle.

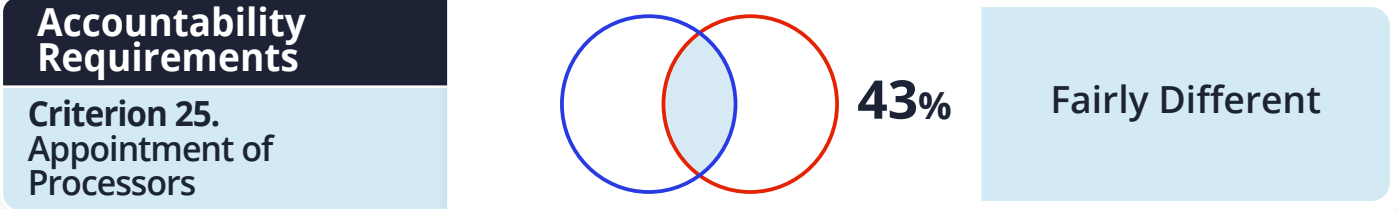
Accountability Requirements**Criterion 24.**
Audit Requirements**Very Different****GDPR****Article 28, 39, 47**



Audits are not mandatory in the GDPR but are presented as a way to monitor GDPR compliance of controllers and processors, or to prove compliance.

Article 54**PIPL**

Personal Information Handlers shall regularly engage in audits of their personal information handling and compliance with laws and administrative regulations.

The PIPL is more stringent in this respect, since it requires Personal Information Handlers to conduct audits of their activities and to comply with applicable laws and administrative rules, whereas the GDPR just encourages non-mandatory audits as a way to monitor or prove compliance.

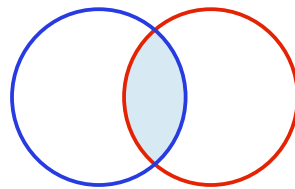


<div> GDPR</div> <div>Article 28</div>	<div>Article 21</div> <div>PIPL </div>
<p>Where processing is to be carried out on behalf of a Data Controller, the Data Controller shall use only Data Processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the Data Subject.</p> <p>The Data Processor shall not engage with another Data Processor without prior specific or general written authorisation of the Data Controller. In the case of general written authorisation, the Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of other Data Processors, thereby giving the Data Controller the opportunity to object to such changes.</p>	<p>Where Personal Information Handlers entrust the handling of personal information, they shall conclude an agreement with the Entrusted Person on the purpose for entrusted handling, the time limit, the handling method, categories of personal information, protection measures, as well as the rights and duties of both sides, etc. Moreover, Personal Information Handlers must conduct supervision of the personal information handling activities of the Entrusted Person.</p> <p>Entrusted Persons shall handle personal information according to the agreement. They may not handle personal information for handling purposes or in handling methods, etc., in excess of the agreement. 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.</p> <p>Without the consent of the Personal Information Handler, an Entrusted Person may not further entrust personal information handling to other persons.</p>

Both the PIPL and the GDPR require an agreement to be signed specifying the aim for entrusting the data, the time limit, the manner of processing, the categories of personal information, the protective measures, and the parties' respective rights and obligations. While the GDPR requires the Data Controller to verify, prior to the processing agreement, that the processor presents sufficient guarantees to meet the GDPR requirements, the PIPL is more strict and requires the Personal Information Handler to conduct supervision of the personal information handling activities of the Entrusted Person.

Accountability Requirements

Criterion 26. Information Security



35%

Fairly Different



GDPR

Article 32

Data Controllers and Data Processors are required to implement appropriate technical and organisational measures to protect the security of personal data, taking into account:

- The state of the art.
- The cost of implementation.
- The nature, scope, context and purpose of processing.
- The risk for the rights and freedoms of natural persons (depending on their likelihood and severity).

Security measures include:

- Pseudonymisation and encryption.
- 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.

Articles 60, 62

PIPL



The State Cybersecurity and Informatization Department is responsible for comprehensive planning and coordination of personal information protection work and related supervision and management work.

Relevant State Council departments, county-level and higher people's government and relevant departments' personal information protection, supervision, and management duties and responsibilities are determined according to relevant State provisions. Those departments are all referred to as departments fulfilling personal information protection duties and responsibilities according to Article 60.

Departments fulfilling personal information protection duties and responsibilities shall set up the following personal information protection duties and responsibilities:

- Conducting personal information protection propaganda 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.
- Other duties and responsibilities provided in laws or administrative regulations.

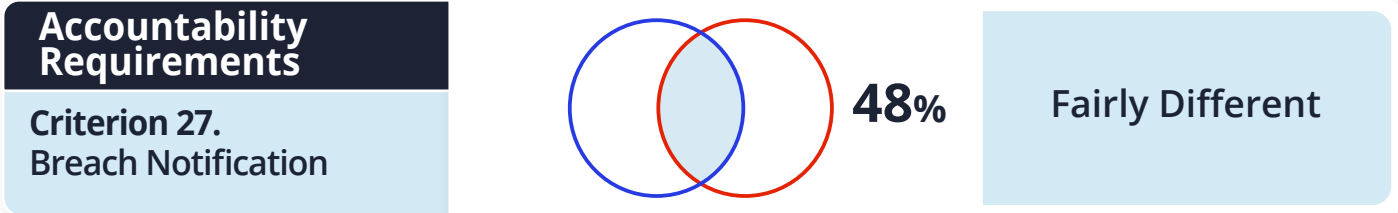
The State Cybersecurity and Informatization Department coordinates overall the following personal information protection work by the relevant departments:

- Formulating concrete personal information protection rules and standards.
- Formulating 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.

- Supporting the research, development, and broad adoption of secure and convenient electronic identity authentication technology, and promoting the construction of public online identity authentication services.
- Advancing the construction of service systems to socialise personal information protection, and supporting relevant organisations to launch personal information protection evaluation and certification services.
- Improving personal information protection complaint and reporting mechanisms.

The PIPL states that the State Cybersecurity and Informatization Department is responsible for the comprehensive planning and coordination of personal information protection work and related supervision and management work, as such, it is more specific than the GDPR, which only claims that Data Controllers and Data Processors are required to implement appropriate technical and organisational measures to protect the security of personal data.

There are two very different cultures concerning the protection of personal information. The GDPR gives more room for manoeuvre to Data Controllers, while under the PIPL, the protection of personal information is part of a national strategy.



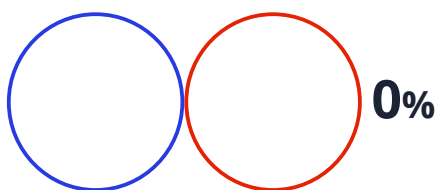
<div>GDPR</div> <div>Article 33, 34</div>	<div>Article 64</div> <div><div>PIPL</div></div>
<p>The GDPR requires the Data Controller to inform without undue delay (and when feasible not later than 72 hours after becoming aware of the breach) the appropriate supervisory authority in the event of a data breach, unless the personal data breach is unlikely to pose a danger to the Data Subject. The Data Processor must notify the Data Controller without undue delay after becoming aware of a personal breach.</p> <p>When a personal data breach is likely to result in a high risk, the Data Controller must inform the Data Subjects implicated as soon as possible.</p> <p>The notification must include at a minimum:</p> <ul style="list-style-type: none">• A description of the nature of the breach, including, where possible, the categories and approximate numbers of Data Subjects affected, as well as the categories and approximate numbers of personal data records affected.• The DPO or another contact point's contact details.• The likely consequences of the breach.• Measures taken or proposed to mitigate the possible adverse effects.• The reason for the breach.	<p>When departments fulfilling personal information protection duties and responsibilities discover in the course of their duties unlawful handling of personal information that is suspected of constituting a crime, they shall promptly transfer the matter to public security authorities for processing according to the law.</p> <p>No further specification is provided by the PIPL, but the Personal Information Security Specification of 2020 recommends Personal Information Handlers notify individuals affected in time, or when the notification is difficult, to release a public alert. The specification also requires the notification to include:</p> <ul style="list-style-type: none">• Details about the security incident and its impact.• Handling measures that have been taken and will be taken.• Recommendations for the Individuals affected to prevent and reduce risks on their own.• Remedial measures provided to Individuals.• Contact information of the person and department responsible for personal information protection.

Both laws have provisions for dealing with data breaches, however, the GDPR's provisions are more thorough.

A breach, according to the GDPR, is defined as "any unauthorised access, modification, or destruction of data". Following a breach, the Data Controller must notify the appropriate supervisory authority immediately. If they are unable to do so within 72 hours from the detection of the breach, they must provide an explanation. If the Data Controller considers the breach poses a significant danger to people's data rights, then the Data Controller must notify the supervisory authority immediately. "High risk" refers to both the probability of injury and the potential for damage.

The PIPL requires notification of competent authorities in the event of a violation, however, there is no time limit in the present law. If there is a danger of harm, the Personal Information Handler must inform impacted persons. Even if they determine that there is no danger of harm, the authorities may force them to notify affected persons.

Criterion 28. Data Localisation Requirements



Different



Articles 5, 44-50

Localisation is not required (unless international data transfer requirements are not met).

Article 40

PIPL



Critical Information Infrastructure Operators and Personal Information Handlers handling personal information at an amount defined by the State Cybersecurity and Informatization Department shall store personal information collected and produced within the borders of the People's Republic of China domestically.

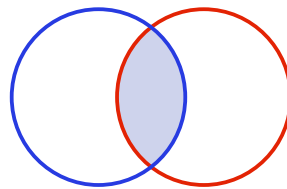
When they need to provide it abroad, they shall pass a security assessment organised by the State Cybersecurity and Informatization Department.

When laws or administrative regulations and the State Cybersecurity and Informatization Department provisions allow the nonexecution of the security assessment, those provisions are to be followed.

Contrary to the GDPR, that does not require special localisation of personal data, the PIPL requires that Critical Infrastructure Information Operators, as well as Entrusted Persons who process personal information that reaches a certain threshold, store personal information within the territory of China.

Data Localisation and Transfer

Criterion 29. International Data Transfer



40%

Fairly Different



Articles 5, 44-50

The GDPR enables personal data to be transferred to a third country or international organisation that meets the EU Commission's criteria for adequate data protection.

In the absence of an EU Commission's adequacy decision, transfers to third countries or international organisations are allowed if it is based on binding appropriate safeguards, including binding corporate rules.

In the absence of an EU Commission's adequacy decision and binding appropriate safeguards, the transfer is authorised, by derogation, in the following cases:

- The Data Subject has explicitly consented to the transfer after having understood the risk of such transfer due to insufficient safeguards.
- The transfer is necessary for the performance of a valid contract between the Data Subject and the Data Controller.
- The transfer is necessary for the conclusion or performance by the Data Controller and other persons of a valid contract that is in the interest of the Data Subject.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for establishment, exercise or defence of legal claims.
- The transfer is necessary to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.
- The transfer (only to the extent laid down by the law) is made from a register which according to the law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.

The transfer is also authorised in an *ad hoc* way if it is not repetitive, concerns a limited number of persons and is necessary for the purposes of compelling legitimate interests pursued by the Data Controller which are not overridden by the interest, rights and freedoms of Data Subjects.

Section 129

PIPL



When Personal Information Handlers truly need to provide personal information outside the borders of the People's Republic of China for business or other such requirements, they must meet one of the following conditions:

- Passing a security assessment organised by the State Cybersecurity and Informatization Department according to data localisation requirements.
- Undergoing personal information protection certification conducted by a specialised body according to provisions by the State Cybersecurity and Informatization Department.
- Concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the State Cyberspace and Informatization Department, agreeing upon the rights and responsibilities of both sides.
- Other conditions provided in laws or administrative regulations or by the State Cybersecurity and Informatization Department.

When treaties or international agreements that the People's Republic of China has concluded or acceded contain relevant provisions such as conditions on providing personal data outside the borders of the People's Republic of China, those provisions may be carried out.

Personal Information Handlers shall adopt necessary measures to ensure that foreign receiving parties' personal information handling activities reach the standard of personal information protection provided in the PIPL.

Both the GDPR and the PIPL impose restrictions on cross-border personal data transfer. However, their provisions are quite different.

Firstly, while the GDPR's preferred mechanism for cross-border personal data transfer is the EU Commission's adequacy decision, the PIPL does not provide for such a mechanism.

Secondly, the GDPR allows cross-border transfers when the Data Controller and the recipient set up binding appropriate safeguards, including standard contractual clauses and binding corporate rules. In the PIPL, the cross-border transfer mechanism must be validated by the State Cybersecurity and Informatization Department. For critical personal information handling, the Personal Information Handler must pass a security assessment. For other cross-border transfers, the Personal Information Handlers can either obtain a personal information certification or conclude a contract with the foreign receiving side in accordance with a standard contract.

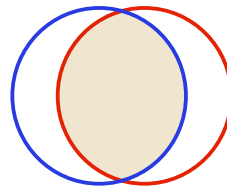
Concerning the different approval mechanisms, the Cyberspace Administration of China (CAC) has released a series of measures to add clarifications. On July 7 2022, the Cyberspace Affairs Commission of China issued the Measures on Security Assessment of Cross-Border Data Transfer (the "Security Assessment Measures"), which sets out the security assessment framework for cross-border data transfers. The Security Assessment Measures will become effective on September 1 2022. In conjunction with the issuance of the Security Assessment Measures, CAC also issued an interpretation guideline on the same day (the "Interpretation Guideline"). The Security Assessment Measures lay out the ground rules for a security assessment filing for cross-border data transfers that was stipulated in the Cybersecurity Law ("CSL") and the Personal Information Protection Law ("PIPL").

And finally, the Cyberspace Administration of China (CAC) released for public consultation on June 30 2022, the template for the Cross-border Data Transfer Agreement, the "Draft China SCC" as part of the "Draft Provisions" on the Prescribed Agreement on Cross-border Data Transfer. The Draft China SCC explains which companies are concerned by this mechanism with a list of conditions, requirements for additional procedures and the contents required in the contract.

Thirdly, even though the GDPR provides derogation and *ad hoc* mechanisms for cross-border transfers, the PIPL does not provide such mechanisms. However, the PIPL provides that other conditions can be provided by law, administrative regulations, and by the State Cybersecurity and Informatization Department.

Enforcement

Criterion 30. Data Protection Authority



68%

Fairly Similar



Articles 31, 51-59

The supervisory authorities have the jurisdiction to:

- Require the Data Controller or Data Processor to bring processing activities into accordance with the GDPR's rules, when applicable, in a particular way and within a set term.
- Apply a temporary or permanent restriction, such as a processing prohibition.

In accordance with EU or Member State procedural law, the supervisory authorities have the authority to:

- Order the Data Controller and Data Processor to provide any information required for the performance of their tasks.
- Obtain access to any premises of the Data Controller and Data Processor, including any data processing equipment and means.

The supervisory authorities also have the jurisdiction to reprimand and give warnings, and to require the correction or deletion of personal data, and apply administrative penalties.

The supervisory authorities have investigative rights, including the ability to conduct data protection audits, evaluate issued certificates, and alert the Data Controller or Data Processor of a suspected GDPR violation.

The GDPR explicitly states that each supervisory authority must carry out its responsibilities and wield its powers independently.

The GDPR is silent on the source of funds that must be made available to regulatory bodies. In this case, the Member State has complete choice over the source of financing.

Articles 60, 65



Organisation

The PIPL states that the State Cybersecurity and Informatization Department is responsible for comprehensive national planning and coordination of personal information protection work and related supervision and management work.

Under the State Cybersecurity and Informatization Department, State Council departments, as well as county-level and higher people's government departments, are responsible for the personal information protection, supervision, and management work within their respective scope of duties and responsibilities. They are referred to as "departments fulfilling personal information protection duties and responsibilities".

Powers and responsibilities

The State Cybersecurity and Informatization Department is responsible for:

- The formulation of concrete personal information rules and standards, including a specialised standard about new technology and new applications.
- Supporting the research, development and broad adoption of secure and convenient electronic identity authentication technology.
- Orchestrating the socialisation of personal information protection, in particular through supporting organisations for evaluation and certification services.
- Perfecting personal protection complaints and reporting work mechanisms.

The departments fulfilling personal information protection duties and responsibilities are responsible for:

- Conducting personal information protection propaganda and education as well as guiding and supervising Personal Information Handlers' conduct of personal information protection work.
- Handling personal information protection-related complaints and report

- Organising evaluation of personal information protection situations, such as procedures used, and publishing the evaluation results.
- Investigating and dealing with unlawful personal information handling activities.
- Other duties and responsibilities provided in laws or administrative regulations.

Both the GDPR and the PIPL impose restrictions on cross-border personal data transfer. However, their provisions are quite different.

Firstly, while the GDPR's preferred mechanism for cross-border personal data transfer is the EU Commission's adequacy decision, the PIPL does not provide for such a mechanism.

Secondly, the GDPR allows cross-border transfers when the Data Controller and the recipient set up binding appropriate safeguards, including standard contractual clauses and binding corporate rules. In the PIPL, the cross-border transfer mechanism must be validated by the State Cybersecurity and Informatization Department. For critical personal information handling, the Personal Information Handler must pass a security assessment. For other cross-border transfers, the Personal Information Handlers can either obtain a personal information certification or conclude a contract with the foreign receiving side in accordance with a standard contract.

Concerning the different approval mechanisms, the Cyberspace Administration of China (CAC) has released a series of measures to add clarifications. On July 7 2022, the Cyberspace Affairs Commission of China issued the Measures on Security Assessment of Cross-Border Data Transfer (the "Security Assessment Measures"), which sets out the security assessment framework for cross-border data transfers. The Security Assessment Measures will become effective on September 1 2022. In conjunction with the issuance of the Security Assessment Measures, CAC also issued an interpretation guideline on the same day (the "Interpretation Guideline"). The Security Assessment Measures lay out the ground rules for a security assessment filing for cross-border data transfers that was stipulated in the Cybersecurity Law ("CSL") and the Personal Information Protection Law ("PIPL").

And finally, the Cyberspace Administration of China (CAC) released for public consultation on June 30 2022, the template for the Cross-border Data Transfer Agreement, the "Draft China SCC" as part of the "Draft Provisions" on the Prescribed Agreement on Cross-border Data Transfer. The Draft China SCC explains which companies are concerned by this mechanism with a list of conditions, requirements for additional procedures and the contents required in the contract.



Thirdly, even though the GDPR provides derogation and *ad hoc* mechanisms for cross-border transfers, the PIPL does not provide such mechanisms. However, the PIPL provides that other conditions can be provided by law, administrative regulations, and by the State Cybersecurity and Informatization Department.

Enforcement

Criterion 31. Penalties

50%

Fairly Similar

<div> GDPR</div> <div>Article 83</div>	<div>Articles 66, 69, 70</div> <div>PIPL </div>
<p>Supervisory bodies may issue rules that include additional factors for calculating the monetary penalty amount. The GDPR allows for sanctions to be imposed on government entities. The creation of laws for the application of administrative fines to public agencies and organisations is left to Member States.</p> <p>Depending on the infraction, the penalty may be:</p> <ul style="list-style-type: none">• Up to 2% of worldwide annual revenue or €10 million, whichever is greater.• 4% of global annual turnover or €20 million, whichever is greater.	<p>In case of non-compliance, the departments fulfilling personal information protection duties and responsibilities 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.</p> <p>In case the circumstances of the unlawful acts are serious, provincial or higher-level departments fulfilling personal information protection duties and responsibilities are to order correction, confiscate unlawful income, and impose a fine or not. The fine may reach more than CN¥50 million or 5% of annual revenue.</p> <p>If the Personal Information Handler refuses to comply, a fine of not more than ¥1 million is to be additionally imposed.</p> <p>They may also order the suspension of related business activities or cessation of business for rectification, and report to the relevant competent department for cancellation of corresponding administrative licences or cancellation of business licences. The directly responsible person in charge and other directly responsible personnel are to be fined between ¥100,000 and ¥1 million, and it may also be decided to prohibit them from holding positions of director, supervisor, high-level manager, or personal information protection officer for a certain period.</p> <p>When 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 take responsibility for the infringement.</p> <p>The responsibility to compensate for infringement shall be determined according to the individual's resulting loss or the Personal Information Handler's resulting benefits. When the individual's loss and the Personal Information Handler's benefits are difficult to determine, compensation shall be determined according to practical conditions.</p> <p>When 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,</p>

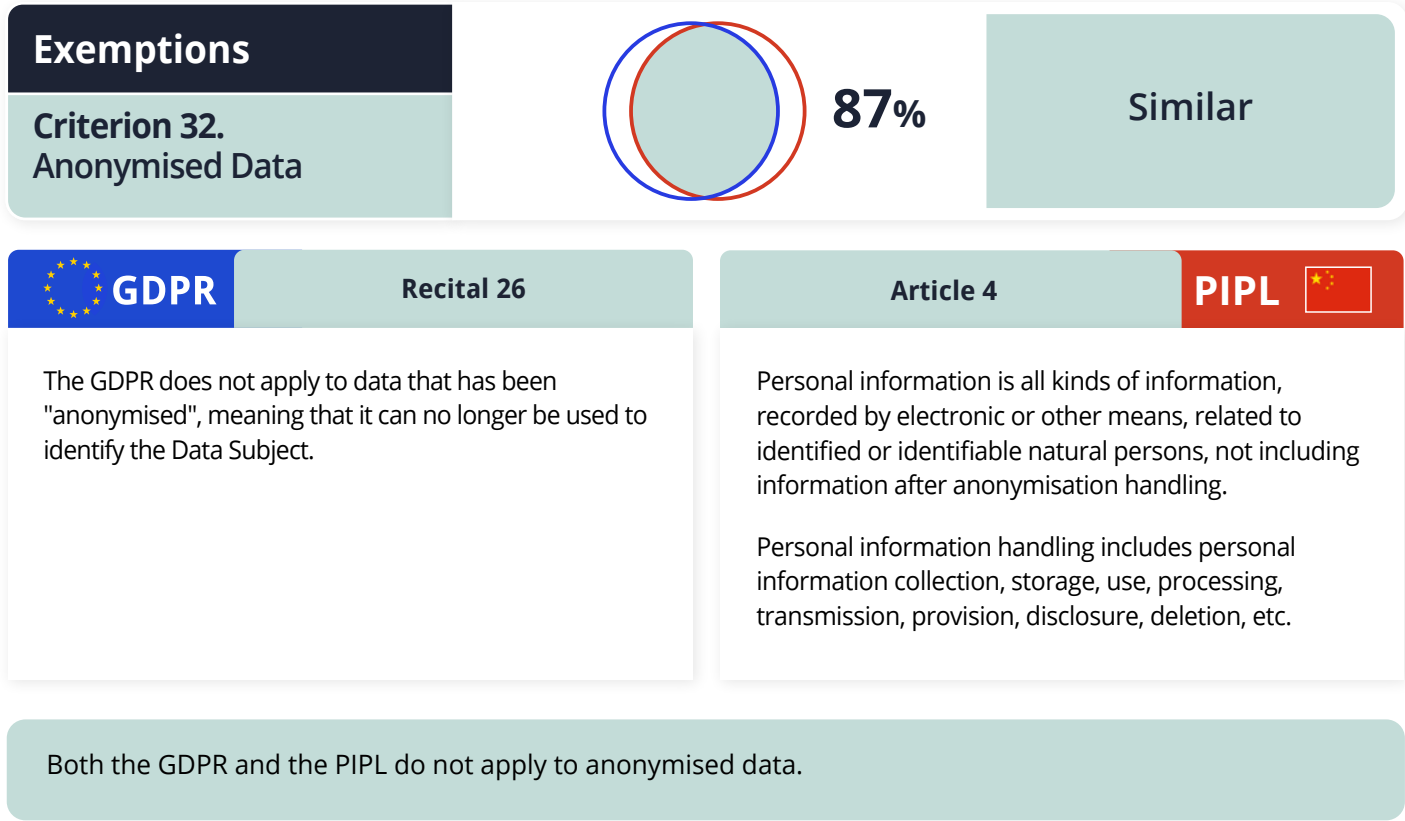
statutorily designated consumer organisations, and organisations designated by the State Cybersecurity and Informatization Department may file a lawsuit with a People's Court according to the law.

Both the GDPR and the PIPL impose enhanced penalties for violations of the law.

Those fines may reach up to 4% of global annual turnover or €20 million under the GDPR and up to CN¥50 million (approximately €7.04 million), or 5% of annual revenue in the PIPL.

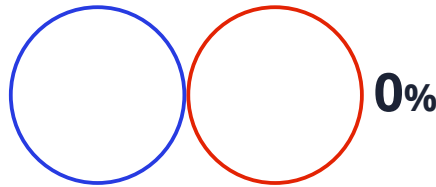
Contrary to the GDPR, the PIPL also provides fines for liable individuals and sanctions that may be related to their career. For example, they may be restricted from serving as a director, supervisor, senior management or personal information protection officer for a stipulated period of time.

The GDPR does, however, state that it leaves it up to the EU Member States to create laws for the application of administrative fines to public agencies and organisations.



Exemptions

Criterion 33. Social Media Intermediaries and Identity Management



Different



There is no mention of requirements for social media intermediaries in the GDPR.

Article 58



Personal Information Handlers providing important Internet platform services that have a large number of users, and whose business models are complex, shall fulfil the following obligations:

- Establish and complete personal information protection compliance systems and structures according to State regulations.
- Establish an independent body composed mainly of outside members to supervise personal information protection circumstances.
- Abide by the principles of openness, fairness, and justice.
- Formulate platform rules; and clarify the standards for intra-platform product or service providers' handling of personal information and their personal information protection duties.
- Stop providing services to product or service providers on the platform that seriously violate laws or administrative regulations in handling personal information.
- Regularly release personal information protection social responsibility reports, and accept society's supervision.

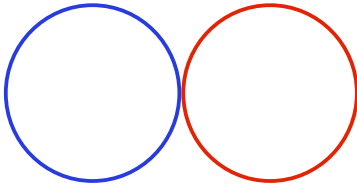
The GDPR does not give any information about social media platforms, contrary to the PIPL that details the obligations for Personal Information Handlers providing important Internet platform services, that have a large number of users, and whose business models are complex.

Those obligations include establishing a compliance and security system whose structure follows State regulations, establishing an independent body composed of outside members to supervise personal information protection circumstances, formulating platform rules, and making the standards clear for intra-platform product or service providers handling personal information. Those platforms also have to cease professional relationships with product or service providers on the platform that seriously violate laws or administrative regulations in handling personal information and regularly release personal information protection social responsibility reports, and accept society's supervision.

Lastly, they must abide by the principles of openness, fairness, and justice.

Exemptions

Criterion 34.
Exemptions for Research



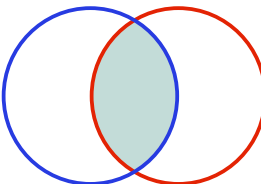
0%

Different

Contrary to the GDPR, the PIPL does not mention any derogation or exemption for research purposes.


Exemptions

Criterion 35.
Application to Public Authorities



50%


Fairly Similar

 **GDPR**

Article 2

The GDPR is not applicable to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

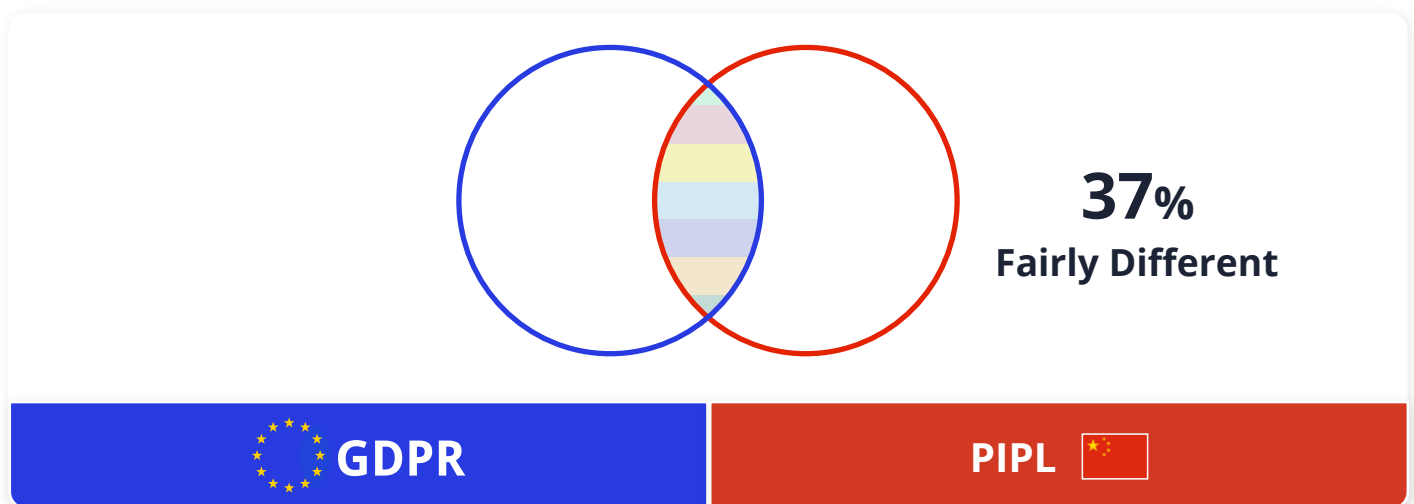
Article 37

PIPL 

The provisions of the PIPL regarding personal information handling by State Institutions apply to the handling of personal information in order to fulfil statutory duties by organisations authorised by laws and regulations to manage public affairs functions.

Contrary to the GDPR, the PIPL does not exempt from its scope State Institutions handling personal information for law enforcement purposes.

Conclusion



While the GDPR and the PIPL share some similarities, they are far from perfectly overlapping. European and GDPR-compliant companies will be familiar with most of the concepts provided by the PIPL, but they will have to consider carrying out a careful gap analysis in order to adapt their structure and measures put in place. Indeed, the PIPL presents different views from the GDPR on several aspects such as consent, Data Processors (Entrusted Persons in the PIPL), data localisation, audit requirements, cross-border transfers, etc. Such a gap analysis is all the more important because the PIPL significantly increased fines for non-compliance, which can be calculated according to the annual turnover of the company.

Moreover, companies processing personal data should not be satisfied with the study of the PIPL as many other relevant laws and regulations can apply, for instance, the Cybersecurity Law and the Data Security Law. Sector-specific regulations are also to be examined as the Anti-Monopoly Law is expected to be updated in 2022, and the regulation on recommended algorithms came into effect on 1 March 2022.

Compliance with the PIPL has been particularly challenging as the PIPL became effective less than three months after its adoption (while the GDPR entered into force two years after its adoption). Further guidance and standards are also expected in order for companies to have a better understanding of the Chinese data protection framework.

Compliance-as-Code: Our Solution

As this report highlights, there is a growing list of data protection compliance requirements around the world, with new laws and legislative requirements in place to assess how personal data or PII (Personal Identifiable Information) is being managed by companies.

Compliance is critical to every business: if you are not compliant with industry regulations, at best, you risk a fine and a bad reputation amongst your ecosystem and customers. At worst, you could be forced to shut your doors and stop trading completely.

At ALIAS, we work with companies and organisations of all sizes to help build in a compliance-as-code approach. Our APIs enable automated compliance: our PII Storage Duration API, for example, regularly assesses stored datasets to ensure that they meet regulatory requirements for the length of time data can be stored by a company.

By implementing compliance at the code level, you are able to automate regulatory prevention and monitoring, in order to increase your compliance coverage over time to 100%, with real-time feedback, and maintain oversight at 100%. This is what we call the DevRegOps approach.

In terms of Data Protection, what is Compliance-as-Code?

Data protection compliance-as-code refers to the tools and practices that allow you to embed the three core activities at the heart of compliance, at the code level of your organisation's tech stack:

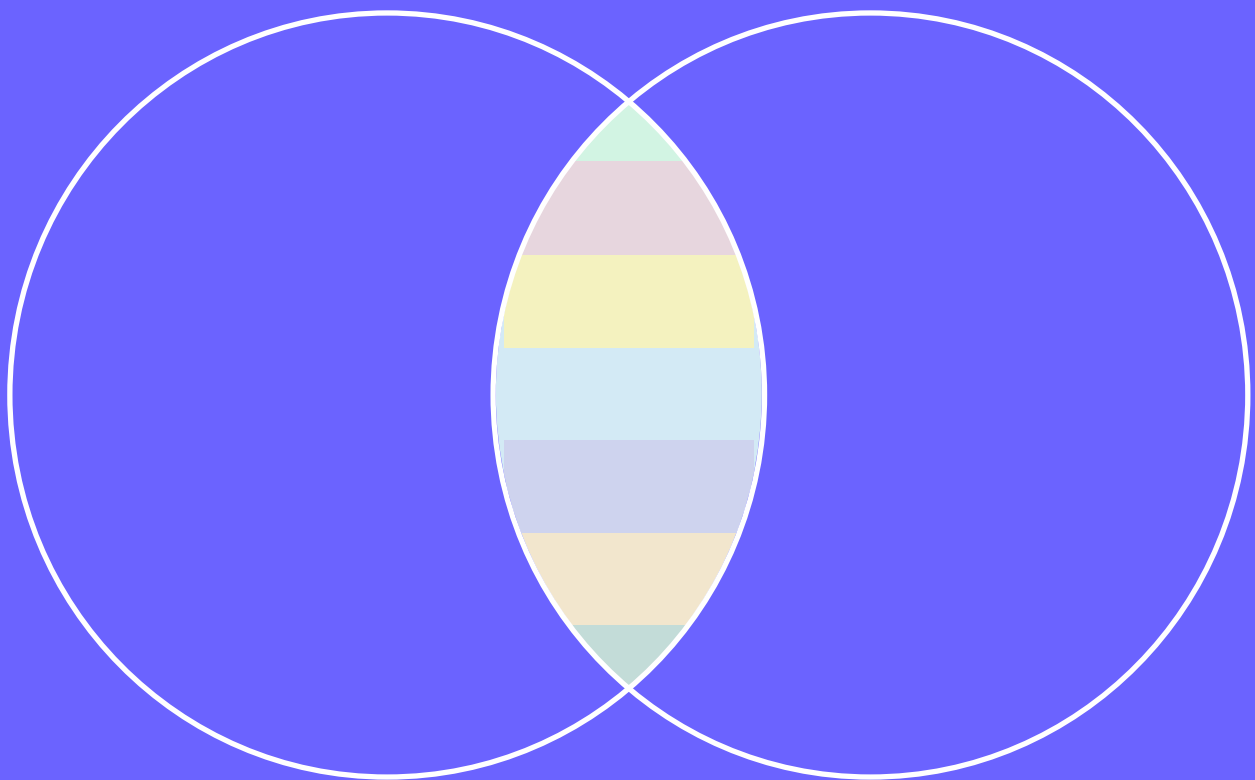
✓ Detect

✓ Solve

✓ Prevent

Contact us for a demo of our tools and to discuss implementing compliance-as-code solutions for your business.

Sign up to our [privacy newsletter](#) to receive information about changing legislations and news regarding data privacy protections.



www.gdpr.dev