Comparing privacy laws: GDPR v. CSL and Specification

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

瑛明律师事务所
Chen & Co. Law Firm

About the authors

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

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

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

Chen & Co. Law Firm: Founded in 1998, Chen & Co. Law Firm is registered to practice the laws of the People's Republic of China in mainland China and Hong Kong. With more than 170 professionals in our Shanghai head office and Beijing, Shenzhen and Hong Kong offices, Chen & Co. Law Firm is widely recognised as a leading commercial law firm in China, uniquely positioned to provide multi-disciplinary, comprehensive legal services to our clients, with particular expertise in capital markets, investment and mergers and acquisitions, anti-trust and corporate compliance legal services. Chen & Co. Law Firm data protection team has helped local and international clients in setting up data protection compliance programs in China, as well as across the globe through the assistance of EY member firms worldwide.

Contributors

OneTrust DataGuidance™
Angus Young, Angela Potter, Holly Highams, Victoria Ashcroft, Tooba Kazmi, Kortyna Kerpauskaite, Emily Dampster, Keshawna Campbell, Theo Stylianou, Andrew Filis, Alexis Kateifides

Chen & Co. Law Firm
Galaad Delval, Dr. Lin Zhong

Image production credits:

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

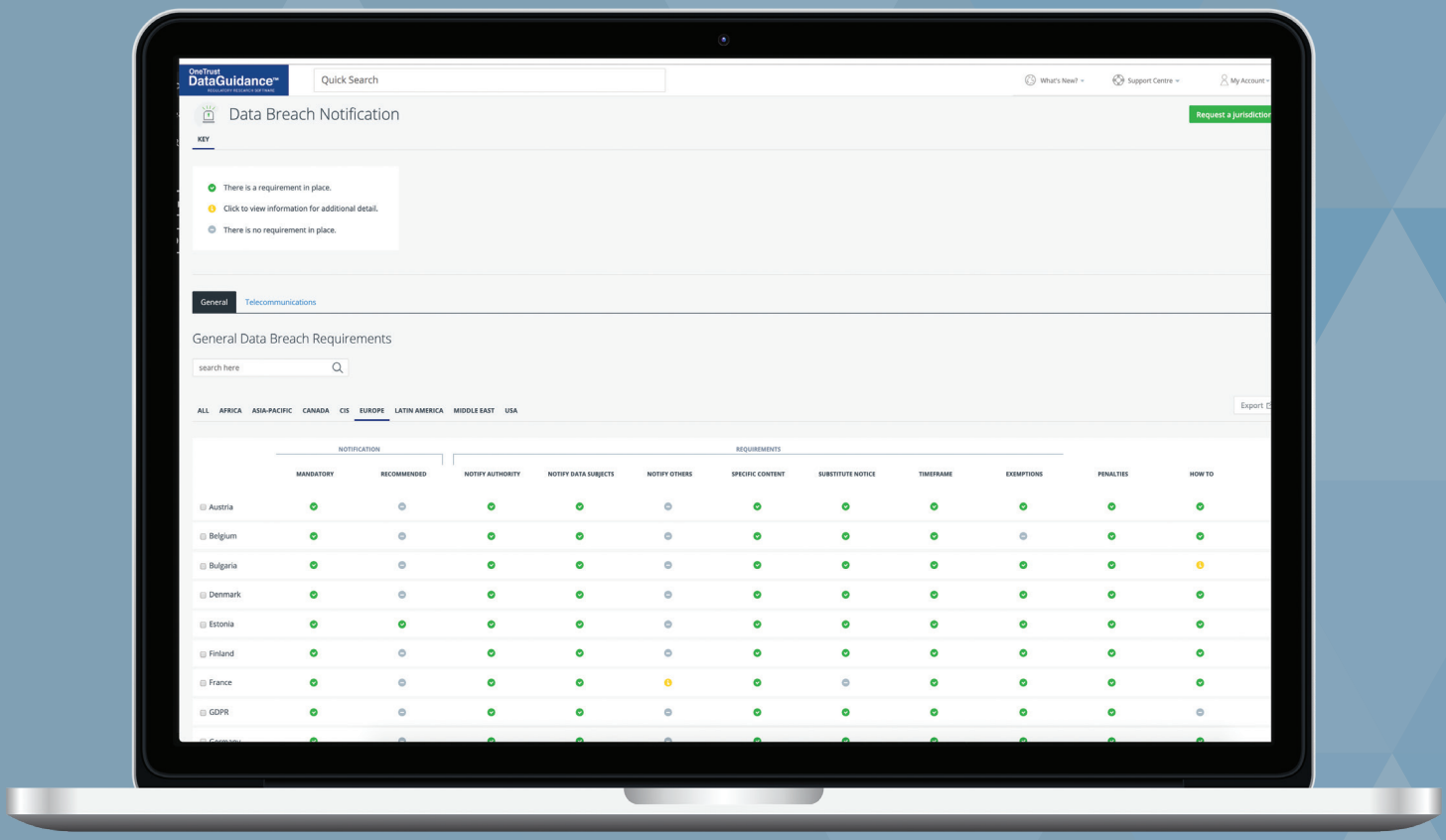
Table of contents

Global Regulatory Research Software

40 In-House Legal Researchers
500 Lawyers Across 300 Jurisdictions

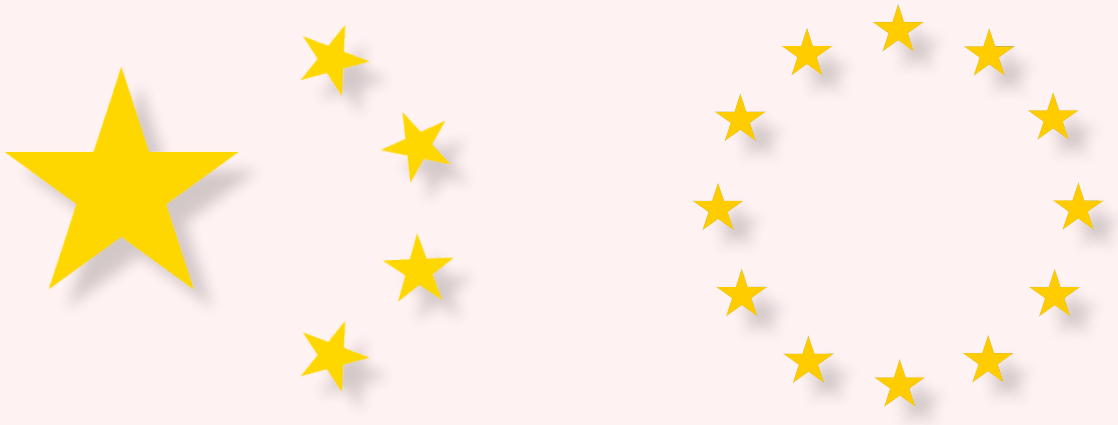
With focused guidance around core topics, Comparison Charts, a daily customised news service and expert analysis, OneTrust DataGuidance provides a cost-effective and efficient solution to design and support your privacy program

- Legal Guidance & Opinion
- Law Comparison Tools
- Breach & Enforcement Tracker
- Ask-An-Analyst Service



SCAN TO ACCESS
FREE TRIAL
Use your camera or a QR code reader

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE



Introduction

On 1 June 2017, the Cybersecurity Law of the People's Republic of China ('CSL') entered into effect in the People's Republic of China ('PRC'). On 25 May 2018, the General Data Protection Regulation (Regulation (EU 2016/679) ('GDPR') entered into force for all European Union ('EU') Member States. The focus of the CSL is national security, cyberspace sovereignty, and the protection of lawful rights and interests. In comparison, the GDPR is principally aimed at the protection of personal data and the regulation of its use. While there are several differences between the two, they both contain provisions governing the processing of personal information; which is defined as 'personal data' under the GDPR and as 'personal information' under the CSL.

Key areas where the CSL contains similar provisions to the GDPR are in relation to the right to be informed, the issuance of monetary penalties and other enforcement actions, and data security. The two significantly differ, though, in areas such as material scope, data transfers, impact assessments, and data protection officer ('DPO') appointments.

In addition to the CSL, there are several other binding regulations in the legislation of the PRC that relate to the protection of personal information. The most notable of these are the Children's Personal Information Network Protection Regulations, which came into effect on 1 October 2019, and the Advertisement Law, as amended with effect on 26 October 2018, which provides relevant restrictions for direct marketing. There are also many administrative regulations that contain sector-specific provisions on personal information protection, but these will not be the subject of this Guide.

Furthermore, there are several non-binding recommendations and standards that have been released by Chinese authorities on cybersecurity and data protection. The most significant of these in the field of data protection is Standard GB/T 35273-2020 on Information Security Technology – Personal Information Security Specification ('the Specification'). The Specification has been recently updated from its 2017 version and a finalised version, which was released on 6 March 2020, will come into effect on 1 October 2020. This Report uses this latest version of the Specification. It should be noted that while these recommendations are not binding and do not have the force of law, they do provide guidance as to best practice regarding the processing of personal information.

While the CSL differs in many ways from the GDPR, the Specification recommends practices that are often close to the GDPR. For instance, the Specification details similar personal information subject rights, definitions for personal and sensitive information, and recommendations for agreements between personal information controllers and entrusted parties (a concept similar to the GDPR's 'data processor').

This Guide principally highlights similarities and differences between the GDPR and the CSL, as well as the GDPR and the Specification. The Guide also specifies where other pieces of Chinese legislation have a relevant, direct, and notable impact. This comparison is intended to help navigate the complex nature of Chinese legislation, and to assist organisations in complying with the GDPR as well as with requirements in mainland China (excluding any other jurisdiction).

Structure and overview of the Guide

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

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

Each topic includes relevant provisions from the two legislative legal frameworks, a summary of the comparison, and a detailed analysis of the similarities and differences between the GDPR and the CSL as well as the Specification.

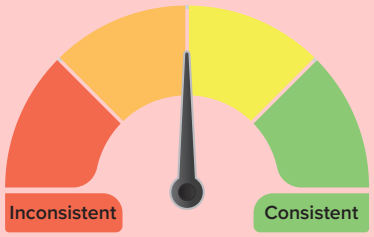
Key for giving the consistency rate

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

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

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

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



Usage of the Guide

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

1. Scope

1.1. Personal scope

CSL
Fairly consistent

Specification
Fairly consistent

Both the GDPR and the CSL protect the processing of personal data/information of natural persons (individuals). In addition, the GDPR states that data protection is provided regardless of the nationality or residency of the data subject, whilst the CSL does not explicitly address this point. However, during the drafting of the CSL, the previous usage of the term 'citizen' to describe the personal information subject was replaced by the term 'natural person,' which suggests that the CSL is intended to provide general data protection coverage. Similarly, the Specification does not precisely address the question of the nationality or residency of the personal information subject.

Both the GDPR and the CSL apply to data controllers and data processors. The CSL, though, does not differentiate between controllers and processors, and applies instead to all 'network operators'. The Specification applies to personal information controllers, and only briefly mentions personal information processors under the term 'entrusted party.'

Please note that the CSL provides binding legal requirements, while the Specification only provides recommendations.

GDPR	CSL Articles 2, 76
Articles 3, 4 Recitals 2, 14, 22-25	Specification Articles 1, 3.3-3.4

Similarities with the CSL

The GDPR **only** protects **living individuals**. The GDPR does not protect the personal data of deceased individuals, this being left to EU Member States to regulate. The GDPR clarifies that a **data subject** is 'an identified or identifiable natural person.'

Article 76.5 of the CSL defines **personal information** as information that can identify a **natural person's** personal identity. There is no explicit mention of deceased individuals in the CSL.

The GDPR **applies** to data controllers and data processors who may be **public bodies**.

Article 2 of the CSL applies to the **construction, operation, maintenance**, and use of **networks** as well as activities which **supervise** and **administer** cybersecurity within the territory of the PRC. The CSL **does not explicitly establish public bodies** as being network operators, however, there are several obligations imposed on cybersecurity authorities throughout the legislation.

Similarities with the Specification

The GDPR **only** protects living individuals. Legal persons' data is not covered by the GDPR. The GDPR **does not** protect the personal data of deceased individuals, this being left to EU Member States to regulate.

Article 1 of the Specification states that the purpose of the text is to protect personal information processing, which, when interpreted with the definition of personal information in Article 3.1 of the Specification, indicates that **only** natural persons are to be protected. The Specification **does not** cover the personal information of deceased individuals.

GDPR	CSL Specification

Similarities with the Specification (cont'd)

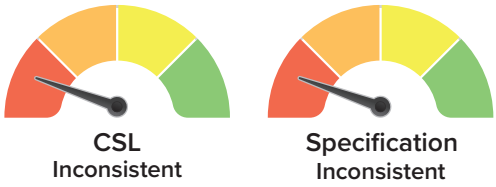
Article 4(1) of the GDPR clarifies that a **data subject** is 'an identified or identifiable natural person.'	Article 3.3 of the Specification clarifies that a **personal information subject** is the 'natural person' identified or related to the personal information.
The GDPR applies to data controllers and data processors who may be **businesses, public bodies, institutions**, as well as **not-for-profit organisations**.	Article 1 of the Specification defines its scope as applying to '**all types of organisations**,' as well as to the '**supervision, management and evaluation of personal information processing activities by competent authorities, third party evaluation agencies and other organisations**.' However, the Specification cannot be interpreted as applying to public authorities and bodies.
The GDPR defines a **data controller** as 'the natural and legal person, public authority, agency or other body which, alone or jointly, with others, determines the purposes and means of the processing of personal data.'	Article 3.4 of the Specification defines a **personal information controller** as 'an organisation or an individual with the right to determine the purpose and means, etc., of personal information processing.'

Differences with the CSL

The GDPR provides that it 'should apply to natural persons, **whatever their nationality or place of residence**,' in relation to the processing of their personal data.	The CSL **does not** contain any explicit provisions on nationality or place of residence for the application of the law outside of the PRC. By following the interpretation of the CSL and the replacement of the term 'citizen' with 'natural person', it can be considered that the CSL applies to any natural person in the PRC **whatever their nationality or place of residence**.
The GDPR defines a **data controller** as a 'natural and legal person, public authority, agency or other body which, alone or jointly, with others, determines the purposes and means of the processing of personal data.' The GDPR defines a **data processor** as a 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'	While the CSL does not define or distinguish between data controllers and data processors, it imposes obligations on **network operators** which are defined under Article 76.3 as 'network owners, administrators, and network service providers.'

GDPR	CSL Specification
Differences with the Specification	
The GDPR provides that it 'should apply to natural persons, **whatever their nationality or place of residence**, in relation to the processing of their personal data.'	The Specification **does not specifically** state that it applies to any natural person, however by following the interpretation of the CSL and the replacement of the term 'citizen' with 'natural person', it can be considered that the Specification applies to any natural person in the PRC **whatever their nationality or place of residence**.
The GDPR defines a **data processor** as a 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.'	The Specification **does not** provide a definition of 'personal information processor,' although it includes a provision on the relationship between personal information controllers and their 'entrusted party' for processing personal information (see section 2.3, below).

1.2. Territorial scope



Both the GDPR and the CSL apply to entities which operate in their respective jurisdictions. The GDPR applies to organisations that have an 'establishment' in the EU, whilst the CSL applies to the construction, operation, maintenance, and use of networks as well as the supervision and administration of cybersecurity within the territory of the PRC.

Only the GDPR, however, has extraterritorial scope. In particular, it applies to organisations that offer goods and services to data subjects in the applicable EU Member States, regardless of where such organisations are located. It should also be noted that only the GDPR applies to organisations that monitor the behaviour of individuals in the EU, regardless of whether they have a presence in the EU.

The Specification does not contain information about its territorial scope, and, as such, it should be understood, similarly to the CSL, as applying solely to the territory of the PRC.

Please note that the CSL provides binding legal requirements, while the Specification only provides recommendations.

GDPR	CSL Article 2, 75
Articles 3, 4, 11 Recitals 2, 14, 22-25	Specification

Similarities with the CSL

GDPR	CSL
The GDPR **applies** to organisations that have a presence in the EU. In particular under Article 3, the GDPR applies to entities that have an '**establishment**' in the EU or if processing of personal data takes place in the context of the activities of that establishment, irrespective of whether the data processing takes place in the EU.	Article 2 of the CSL outlines that it applies to the **construction, operation, maintenance and use of networks**, as well as the **supervision and administration of cybersecurity within the territory of the PRC**.

Similarities with the Specification

GDPR	CSL
Not applicable.	Not applicable.

Differences with the CSL

GDPR	CSL
In relation to **extraterritorial scope**, the GDPR applies to the processing activities of data controllers and data processors that **do not have any presence in the EU**, where processing activities are related to the **offering of goods or services to individuals in the EU, or to the monitoring of the behaviour of individuals in the EU**.	The CSL does not explicitly exclude extraterritorial application, however it is **understood not to have extraterritorial application** beyond Article 75 (on investigating an overseas organisation, institution, or individual engaged in any activity endangering critical information infrastructure of the PRC).

GDPR	CSL Specification

Differences with the Specification

The GDPR applies to the processing of personal data by organisations **established** in the EU, regardless of **whether the processing takes place in the EU**. The GDPR also contains provisions for its **extraterritorial scope**.

The Specification **does not** provide information about its territorial scope. As such, it should be understood as following the territorial scope of the CSL, and therefore personal information processing on networks within the territory of the PRC.

1.3. Material scope

CSL
Fairly inconsistent

Specification
Fairly consistent

Both the GDPR and the CSL apply to personal data/information, which is defined as any information related to an identified or identifiable natural person. The GDPR excludes from its application the processing of anonymous data. Similarly, the CSL creates an exemption allowing network operators to, without the consent of the personal information subject, further process personal information that has been 'anonymised.'

The GDPR applies to the processing of personal data by automated means or non-automated means if the data is part of a filing system. In comparison, the CSL applies to any processing occurring on a network while carrying out business and service activities. Generally, the material scope of the Specification follows that of the CSL.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL Articles 2, 9, 42, 76
Articles 2-4, 9 Recitals 15-21, 26	Specification Articles 1, 3.1-3.2, 3.14, 5.6

Similarities with the CSL

The GDPR defines **'personal data'** as 'any information' that directly or indirectly relates to an identified or identifiable individual.

Article 76.5 of the CSL defines **personal information** as 'all kinds of information electronically or otherwise recorded that can independently or combined with other information be used to identify a **natural person**.'

The GDPR excludes **anonymous data** from its application, which is defined as information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The CSL does not explicitly refer to anonymous data. However, Article 42 of the CSL provides that personal information may not be provided to others without the agreement of the user whose information is being collected, **except where it has been processed in such a manner that it is impossible to identify a particular individual and the information cannot be recovered**.

Similarities with the Specification

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

Article 1 of the Specification provides that it applies to the **processing** of personal information. While the term 'processing' is not explicitly defined in the Specification, it can be understood through the interpretation of Article 1 as the 'collection, preservation, use, sharing, transfer, disclosure, etc.' of personal information.

GDPR	CSL Specification

Similarities with the Specification (cont'd)

The GDPR applies to the **processing** of personal data. '**Personal data**' is defined as 'any information' that directly or indirectly relates to an identified or identifiable individual.	Article 1 of the Specification provides that it applies to the **processing** of personal information. '**Personal information**' is defined in Article 3.1 of the Specification as 'all kinds of information electronically or otherwise recorded that can independently or combined with other information be used to identify a natural person.'
The GDPR defines '**special categories of personal data**' as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The GDPR provides specific requirements for processing such data.	Article 3.2 of the Specification defines '**personal sensitive information**' as 'personal information that once disclosed, illegally provided or misused, may endanger personal and property safety, easily lead to personal reputation, physical or mental health damage or discriminatory treatment.' The Specification has higher requirements for the processing of personal sensitive information.
The GDPR excludes from its application the processing of **personal data by individuals for purely personal or household purposes**. This is data processing that has 'no connection to a professional or commercial activity.'	The Specification **does not explicitly** exclude from its application the processing of personal information by individuals for purely personal or household purposes. **However, when interpreting the Specification in light of Article 9 of the CSL**, such activity would be excluded from the scope of the Specification.
The GDPR excludes **anonymous data** from its application, which is defined as information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.	Article 3.14 of the Specification does not apply to **anonymised information**, which is information that has been through a technical process that prevents the use of the information to identify a natural person, and that cannot be reversed. Article 3.14 of the Specification explicitly states that such anonymised information should not be regarded as personal information.
The GDPR provides specific requirements for certain processing situations, including processing for **journalistic purposes and academic, artistic or literary expression**.	Articles 5.6(j) and 5.6(k) of the Specification provide specific requirements for certain processing situations, such as **journalistic and academic research purposes**. However, processing of personal information for **artistic or literary purposes is not covered** by the Specification.

GDPR	CSL Specification
Differences with the CSL	
The GDPR **defines** 'processing' as 'any operation' performed on personal data 'such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.'	The CSL **does not define 'processing'** of personal information.
The GDPR **excludes** from its application data processing in the context of **law enforcement** or **national security**.	The CSL **does not** explicitly exclude data processing in the context of law enforcement or national security.
The GDPR defines **special categories of personal data**. The GDPR also provides specific requirements for its processing.	The CSL **does not differentiate categories** of personal information.
The GDPR provides requirements for specific processing situations including processing for **journalistic purposes and academic, artistic or literary expression**.	The CSL **does not** provide requirements for specific processing situations.
The GDPR applies to the processing of personal data **by automated means or non-automated means if the data is part of a filing system**.	The CSL **does not** refer to or differentiate processing by automated and non-automated means.
The GDPR refers to the protection of fundamental rights and interests. However, the GDPR **does not refer to cybersecurity or cyberspace sovereignty**.	Article 1 of the CSL notes that the CSL is formulated for **the purposes of protecting cybersecurity, safeguarding cyberspace sovereignty, national security and public interests, protecting the lawful rights and interests of citizens, legal persons and other organisations**, and promoting the sound development of economic and social informatisation.
The GDPR **does not** contain references to notions such as social morality, cyberspace, or activities that may endanger national honour.	The CSL provides that individuals and organisations should respect **social morality, and shall not endanger cybersecurity** or use networks to engage in any activities that **endanger national security, national honour**, and **national interests**.

GDPR	CSL Specification
Differences with the Specification	
The GDPR excludes from its application data processing within the context of **law enforcement or national security**.	The Specification does not explicitly exclude from its application personal information processing within the context of law enforcement or national security. However, Article 5.6(b) of the Specification provides an exclusion from consent requirements where processing of personal information is directly related to **national security or national defense security**. Article 5.6(c) of the Specification also provides a similar exception from consent requirements where processing is directly related to **public safety, public health** and **major public interests**, while Article 5.6(d) Specification provides exemptions where processing is directly related to **criminal investigation, prosecution, trials,** or **execution of judgments**.
The GDPR applies to the processing of personal data **by automated means or non-automated means if the data is part of a filing system**.	The Specification **does not** contain equivalent provisions.

2. Key definitions

2.1. Personal data

The GDPR and the CSL provide very similar definitions of personal data/information. While the GDPR also defines anonymised data, the CSL only approaches this concept as an exception to consent without explicitly referring to the term 'anonymised information.' In addition, the GDPR addresses sensitive personal data, which the CSL does not.

The Specification, however, is much closer to the GDPR, with definitions of personal information, personal sensitive information, and anonymised information that are almost in line with the GDPR.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL Articles 42, 76 Specification Articles 3.1, 3.2, 3.14, 5.1, Annexes A and B
Articles 4, 9 Recitals 26-30	

Similarities with the CSL

The GDPR defines '**personal data**' as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

Article 76.5 of the CSL defines '**personal information**' as 'all kinds of information electronically or otherwise recorded that can **independently** or **combined** with other information be used to identity a natural person', including but not limited to a natural person's name, date of birth, ID number, personal biometric information, address, and telephone number.

The GDPR **does not** apply to 'anonymised' data, where the data can no longer be used to identify the data subject.

The CSL does not explicitly refer to anonymous data. However, Article 42 of the CSL provides that personal information may not be provided to others without the agreement of the user whose information is being collected, **except where it has been processed in such a manner that it is impossible to identify a particular individual and the information cannot be recovered**.

Similarities with the Specification

The GDPR, defines '**personal data**' as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,

Article 3.1 of the Specification defines '**personal information**' as 'all kinds of information electronically or otherwise recorded that can independently or combined with other information be used to identity a natural person.' Annex A of the Specification provides a detailed list of categories of personal information.

GDPR	CSL Specification

Similarities with the Specification (cont'd)

location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.'

The GDPR does not apply to **anonymised data**, notably data which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer is identifiable.

The Specification does not apply to **anonymised information**, notably information that has been through a technical process that prevents the use of the information to identify a natural person, and that cannot be reversed. Article 3.14 of the Specification explicitly states that such information should not be regarded as personal information.

The GDPR defines **special categories of personal data** (or 'sensitive data') as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.'

Article 3.2 of the Specification defines '**personal sensitive information**' as 'personal information that once disclosed, illegally provided or misused, may endanger personal and property safety, easily lead to personal reputation, physical or mental health damage or discriminatory treatment.' Annex B of the Specification provides a detailed list of categories of personal sensitive information.

Differences with the CSL

The GDPR defines **special categories of personal data**.

The CSL **does not define special categories of personal information**. Moreover, the CSL **does not make reference** to racial or ethnic origin, religious or philosophical beliefs, trade union membership, or data concerning health, sex life, or sexual orientation. **Biometric data** is **included** in the definition of '**personal information**' and is not classified as a special category.

The GDPR specifies that **online identifiers**, such as **IP addresses, cookie identifiers, and radio frequency identification tags**, may be considered personal data.

The CSL **does not explicitly specify** that online identifiers may be considered personal information, although such information is understood to be covered. (Please note that online identifiers have been considered personal information elsewhere within China's legal system).

GDPR	CSL Specification
Differences with the Specification	
Under the GDPR, the **processing of special categories of personal data ('sensitive data') is prohibited** unless exceptions apply. See section 3 on 'Legal Basis,' below.	Under Article 5.1(e) of the Specification, the **large-scale collection of personal sensitive information** is considered to be a violation of the principle of the legality of processing. For general processing of personal sensitive information, additional requirements must be set in place.
Recital 26 of the GDPR provides that '**to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used**, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.'	The Specification **does not** provide for a means to assess the validity of an anonymisation procedure.

2.2. Pseudonymisation

The GDPR contains a definition of 'pseudonymisation,' while the CSL does not refer to this concept. Furthermore, the GDPR states that pseudonymised data should be regarded as personal data, and notes that the process of pseudonymisation is a safeguard to be taken for reducing risks to the rights of data subjects.

Unlike the CSL, the Specification adopts an approach closer to the GDPR with similar recommendations for the use of 'de-identified information.'

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL
Articles 4, 11 Recitals 26, 28-29	Specification Articles 3.15, 6.2

Similarities with the CSL

Not applicable.

Not applicable.

Similarities with the Specification

'**Pseudonymisation**' is defined in the GDPR as 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.'

Recital 29 of the GDPR recommends that 'measures of pseudonymisation should, whilst allowing general analysis, be possible within the same controller when that controller has taken **technical and organisational measures** necessary to ensure, for the processing concerned, that this Regulation is implemented, and that additional information for attributing the personal data to a specific data subject is kept separately.'

Article 3.15 of the Specification defines '**de-identification**' as 'the technical process through which personal information cannot identify or be associated with the personal information subject without the help of additional information.'

Article 6.2 of the Specification recommends that personal information be the subject of de-identification, that such de-identification should be done immediately after the collection of personal information, and that **technical and management measures** should be implemented to separate information which may allow for re-identification, as well as to strengthen access and user rights management.

GDPR	CSL Specification

Differences with the CSL

The GDPR defines '**pseudonymised data.**'	The CSL **does not define** 'pseudonymised data.'

Differences with the Specification

The GDPR clearly states that 'personal data that have undergone pseudonymisation, and **which could be attributed to a natural person by the use of additional information** should be considered as information on an identifiable natural person.'	The Specification **does not** specifically state whether personal information that has undergone de-identification should be considered as information on an identifiable natural person.

2.3. Controllers and processors

CSL
Fairly inconsistent

Specification
Fairly consistent

The GDPR provides a definition of controllers and processors, while the CSL only defines the term 'network operator,' which would, in principle, include the concepts of data controllers and processors.

Comparatively, the Specification only explicitly provides a definition of personal information controllers. However, the Specification does mention the relationship between a personal information controller and an 'entrusted party.'

The GDPR requires that the relationship between the controller and the processor be governed by a contract or other legal act. As this relationship does not exist in the CSL, only the Specification provides recommendations on how personal information controllers should regulate their relationship with an entrusted party.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL Articles 21, 31, 34, 36-38, 41-43, 76 Specification Articles 3.4, 9.1, 9.2, 11.3
Articles 4, 28, 30, 82	

Similarities with the CSL

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

Under Article 41 of the CSL, network operators who collect and use personal information shall abide by the principles of **legality, propriety, and necessity,** explicitly stating the **purposes, means, and scope** for collecting or using information; network operators **shall not collect** personal information **unrelated** to the services they provide. In addition, network operators shall adopt measures to **correct or delete inaccurate personal information**.

Data controllers must implement **technical and organisational security measures**, and notify supervisory authorities of **data breaches**.

Under Article 21 of the CSL, network operators have several **security protection** duties, including **adopting technical measures** to prevent computer viruses, cyberattacks, network intrusions, and other activities that may endanger cybersecurity. They must also **record cybersecurity incidents**. In addition, under Article 42 of the CSL, **disclosure, damage, or loss** of personal information must be notified to the user and the competent department.

The GDPR stipulates that data controllers and data processors should **keep records of processing activities**, and provides an exception from this obligation for smaller organisations. It also provides for the designation of a **data protection officer** ('DPO') by data controllers or data processors.

Article 21.3 of the CSL provides that network operators must adopt measures to **record** the status of network operations, cybersecurity incidents, and **store relevant network logs for at least six months**. The CSL also requires network operators to determine the **persons in charge of cybersecurity**.

GDPR	CSL Specification

Similarities with the CSL (cont'd)

The GDPR provides that a data controller or data processor conduct **Data Protection Impact Assessments** ('DPIA') in certain circumstances.	Under Article 37 of the CSL, operators of critical information infrastructure ('CII') must conduct a **security assessment** if it is necessary to transfer personal information outside of mainland China.

Similarities with the Specification

A **data controller** is defined in the GDPR as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, **determines the purposes and means of the processing of personal data**; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.'	Article 3.4 of the Specification defines a **personal information controller** as 'an organisation or an individual **with the right to determine the purpose and means, etc., of personal information processing**.'
A **data processor** is defined in the GDPR as 'a natural or legal person, the public authority, agency or any other entity which processes personal data on behalf of the controller.'	The Specification does not define the term 'personal information processor.' However, it contains a provision dedicated to the delegation of processing and the relationship between the personal information controller and the '**entrusted party**' ('受委托者' in the original Chinese). However, the term 'entrusted party' is not defined in the Specification.
Under Article 28(3) of the GDPR, the data processor must process the personal data only on **documented instructions** from the controller which should **detail the scope of the personal data processing, itself in line with the original purpose of the collection** of the personal information.	Article 9.1(a) of the Specification recommends that the scope of the processing done by the entrusted party **should not go beyond what was agreed by the personal information subject with the personal information controller**, or beyond the consent exemption clauses stipulated in Article 5.6 of the Specification.
Under Article 28(1) of the GDPR, the data controller should only select data processors providing **sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing will meet the requirements of the GDPR, and ensure the protection of the rights of the data subject.	Under Article 9.1(b) of the Specification, the personal information controller should conduct a personal information impact assessment on the entrusted party in order to ensure that the latter meets **the Specification's data security capabilities requirements**.
Under Articles 28(1) and 28 (3)(e) of the GDPR, the data processor shall **assist the controller** in implementing appropriate technical and organisational measures, insofar	Under Article 9.1(c)(3) of the Specification, the entrusted party should provide **assistance to the personal information controller when responding to personal information subjects' requests**.

GDPR	CSL Specification

Similarities with the Specification (cont'd)

as this is possible, for the fulfilment of the controller's obligation **to respond to requests for exercising the data subject's rights** laid down in Chapter III.	
Under Articles 28(1) and 28(3)(f) of the GDPR, the data processor **shall assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36** taking into account the nature of processing and the information available to the processor.	Under Article 9.1(c)(4) of the Specification, when a **security incident** occurs in the process of handling personal information, **the entrusted party should provide timely feedback** to the personal information controller.
Under Articles 28(1) and 28(3)(g) of the GDPR, the **data processor shall, at the choice of the data controller, delete or return all the personal data to the controller after the end of the provision of services relating to processing**, and delete existing copies unless Union or Member State law requires storage of the personal data.	Under Article 9.1(c)(5) of the Specification, when the relationship between the personal information controller and the entrusted party is terminated, the latter should **no longer save the relevant personal information**.
A controller or processor is **exempt from liability** if it proves that it is not in any way responsible for the event giving rise to the damage.	In principle, under Article 9.2(g) of the Specification, in case of damage to the legitimate rights and interests of the personal information subject due to a security incident involving sharing and transferring personal information, the personal information controller should bear the **corresponding responsibility**.
Under the GDPR, the controller and the processor shall **maintain a record of the processing activities** under their responsibility.	Article 11.3 of the Specification recommends that the personal information controller, thus including entrusted parties, **establish, maintain and update their record of personal information processing activities**.
The GDPR requires processing by a processor to be governed by **a contract or another legal act** 'that is binding on the processor with regard to the controller and that sets out the subject matter and the duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects and the obligations and rights of the controller.'	Article 9.1(d) of the Specification recommends that the personal information controller supervise the entrusted party, notably through **means of contract**.
Article 26 of the GDPR provides that two data controllers or a data controller and a data processor can be considered to be **joint controllers** for a specific processing under given circumstances.	Article 9.6 of the Specification provides for cases when two personal information controllers can be considered as **common personal information controllers** for a specific processing of personal information.

GDPR	CSL Specification

Differences with the CSL

A **data controller** is a natural or legal person, public authority agency or other body that determines the **purposes** and **means** of the processing of personal data, alone or jointly with others. A **data processor** is a natural or legal person, public authority, agency, or other body which processes personal data on **behalf** of the controller.	The CSL **does not** define 'data controller' or 'data processor.' Instead, the CSL applies to '**network operators**' and '**operators of CII**.' Network operators are defined under Article 76 as network owners, administrators, and network service providers. Operators of CII are broadly defined under Article 31 as the operators of information infrastructure that will result in serious damage to the national security, national economy, and people's livelihood and public interests if that are destroyed, there are lost functions, or they are subject to data leakage.
Data controllers based outside the EU and involved in certain forms of processing, with exceptions related to the scale of processing and type of data, are obliged to **designate a representative based in the EU** in writing.	The CSL **does not** contain any provisions regarding operators based outside the PRC.
The GDPR provides that where processing is to be carried out on behalf of a controller, the **controller shall use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures** in such a manner that processing meets the requirements of the GDPR, and ensures the protection of the rights of the data subject. In addition, the data processor must not engage another data processor (sub-processor) without prior specific or general written **authorisation** of the controller.	While Article 36 of the CSL requires operators of CII to sign a **security and confidentiality agreement** with the service provider from whom it purchases network products and services, which clarifies the operators of CII's obligations, there are no similar provisions for controller and processor agreements.

Differences with the Specification

Under the GDPR, '**any controller involved in the processing shall be liable for the damage caused by the processing which infringes this Regulation**. A processor shall be liable for the damage caused by the processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to the legal instructions of the controller.'	Article 9.1(d)(1) of the Specification recommends that the liability of the personal information controller and the entrusted party be **stipulated by means of contract.**
Under the GDPR, the **concept of a sub-processor is covered** and subject to additional requirements under Article 28.	The Specification **does not** specifically cover the cases of sub-processors.

2.4. Children

CSL
Inconsistent

Specification
Fairly inconsistent

The GDPR grants special protection to children's personal data, but the CSL does not refer to children's personal information. Instead the primary piece of legislation in mainland China specifically governing children's personal information is the Children's Personal Information Network Protection Regulations ('the Children's Regulations'). The Specification recommends that children's personal information should receive a heightened level of protection.

With regard to consent to information society services, the GDPR sets the minimum age at 16 years old, although EU Member States may set a lower age, as long as they abide by a minimum of 13 years of age. Under that age, consent must be given by a parent or legal guardian. Comparatively, both the Children's Regulations and the Specification provide an age threshold of 14 years, and set out particular requirements that apply to personal information subjects under this age.

Please note that the CSL and Children's Regulations contain legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL
Articles 6, 8, 12, 40, 57 Recitals 38, 58, 75	Children's Regulations Articles 2, 9, 10 Specification Articles 3.2, 5.4

Similarities with the CSL or the Children's Regulations

When any information is addressed specifically to a child, controllers must take **appropriate measures** to provide **information** relating to processing in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, that the child can easily understand.

The CSL **does not** refer to information specifically addressed to a child. However, Articles 9 and 10 of the Children's Regulations require that information regarding the processing of children's personal information should be **provided in a clear manner**.

Simiarities with the Specification

Under the GDPR, the minimum age to consent to information society services is **16**, but EU Member States may provide for a lower age for those purposes, provided that such lower age is not below **13**.

Under Article 5.4 of the Specification, the minimum age to consent should be set at **14 years old**. If the individual is under 14, the consent of the guardian is required.

Differences with the CSL or the Children's Regulations

The GDPR **does not** define 'child' nor 'children.'

Article 2 of the Children's Regulations **defines children as under 14 years of age.**

Where the processing is based on consent, the consent of a parent or guardian is required for providing information society services to a child below the **age of 16**. EU Member States can **lower this age limit to 13**.

Neither the Children's Regulations nor the CSL require consent specifically for the provision of information society services. However, Article 9 of the Children's Regulations obliges network operators to

GDPR	CSL Specification

Differences with the CSL or the Children's Requirements (cont'd)

	obtain consent from children's guardians in order to collect, use, transfer, or disclose children's personal information.
The GPDR provides that data controllers are required to make reasonable efforts to **verify** that **consent** is given or authorised by a parent or guardian.	**Neither the CSL nor the Children's Regulations** require specific efforts to verify that consent is given or authorised by a parent or guardian.
The GDPR provides general requirements for personal data processing but **does not** stipulate these requirements in a distinct fashion regarding children's personal data.	The Children's Regulations stipulate several **requirements and relate them specifically to children's personal information**, including, among other things: designating responsible personnel; signed agreements and security assessments for data transfers; measures such as encryption to ensure information security; deleting information in certain circumstances; restricting access to information; obtaining consent for processing; and notifying parents or guardians.

Differences with the Specification

Under the GDPR, children's information **is not** considered a special category of personal data.	Under Articles 3.2 and 5.2(b) of the Specification, the personal information of children under 14 years old **should be considered personal sensitive information.**
The GDPR explicitly addresses children's consent **only in the context of the offering of information society services**.	Article 5.4(d) of the Specification **generally** addresses children's consent for the processing of their personal information. Under Article 5.2(c) of the Specification, **before collecting children's personal biometric information**, the personal information subject or their guardian should be separately informed of the purpose, method, and retention time for the collected information, as well as the collection and use scope of the personal biometric information. Explicit consent should then be collected from the personal information subject or their guardian.
The GDPR states that specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.	The Specification **does not** include equivalent provisions.

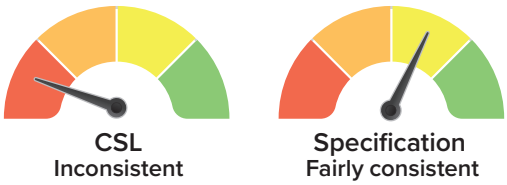
GDPR	CSL Specification

Differences with the Specification (cont'd)

The GDPR requires controllers to make **reasonable efforts** to verify if consent has been given or authorised by a parent/guardian. The GDPR states that any information and communication, addressed to a child, should be provided in such a **clear and plain language** that the child can easily understand.

The Specification **does not** include equivalent provisions.

2.5. Research



The GDPR's provisions on research are more flexible than those of the CSL. The GDPR states that scientific research should be interpreted in a 'broad manner,' while the CSL does not mention research purposes for the processing of personal information.

In regard to the Specification, the purpose of research can be used both to process personal information without consent, as well as to process personal information beyond the original scope of the collection.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL
Articles 5, 6, 9, 14, 17, 89 Recitals 33, 156, 159-161	Specification Articles 5.6(k), 7.3, 8.7(e)(3)

Similarities with the CSL

GDPR	CSL
Not applicable.	Not applicable.

Similarities with the Specification

GDPR	CSL
The GDPR provides that 'further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), **not be considered to be incompatible with the initial purposes**.'	Article 7.3 of the Specification states that the processing of personal information for academic research, or to obtain a description of an overall natural, scientific, economic, and other phenomena statistic can belong to **a reasonable scope related to the original personal information collection purpose**.

Differences with the CSL

GDPR	CSL
According to the GDPR, the **processing of sensitive data is not prohibited when 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes**, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.'	The CSL **does not** provide an exception for the processing of sensitive data when necessary for archiving purposes in the public interest, scientific, or historical research purposes, or statistical purposes.
The GDPR provides that data subjects have the **right to object** to the processing of personal data for research purposes **unless such research purposes are for reasons of public interest**. The GDPR also provides that the processing of personal data for research purposes is subject to **specific rules**, clarifies that the processing of personal data for **scientific research** purposes	The CSL **does not** provide equivalent provisions.

GDPR	CSL Specification

Differences with the CSL (cont'd)

should be interpreted 'in a broad manner,' and that it is possible for EU Member States to derogate from some data subject rights where personal data are processed for research purposes.

Differences with the Specification

The GDPR **does not** provide an exemption to consent for processing related to academic research purposes.

Article 5(6)(k) of the Specification states that processing of personal information for **academic research purpose can be exempted from consent requirements**. However, the Specification **does not** provide a definition of 'academic research purpose.'

According to the GDPR, **the processing of sensitive data is not prohibited when 'necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.'** In addition, special categories of personal data which deserve higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole.

Under the Specification, the processing of **personal sensitive information is in principle not prohibited as long as it is not performed on a mass scale**.

Under the GDPR, where personal data are processed for archiving purposes in the public interest and research purposes, it is possible **for Member States to derogate from some data subject rights**, insofar as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

The Specification does not have such provisions limiting the rights of personal information subjects for research purposes. However, if the exercise of the right is related to processing directly related to **public security, public health, and major public interests**, then the request to exercise such right can be denied under Article 8.7(e)(3) of the Specification.

3. Legal basis

CSL
Fairly inconsistent

Specification
Fairly inconsistent

The GDPR requires a legal basis to be identified in order to lawfully process personal data, while the CSL requires consent to be obtained to process personal information. The CSL by itself does not provide any other legal basis to process personal information.

The Specification provides that consent is the main legal basis to process personal information. However, it also suggests that certain forms of processing of personal information can be considered exempt from consent requirements and details alternate legal bases.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL Article 41
Articles 5-10 Recitals 39-48	Specification Articles 5.4, 5.6

Similarities with the CSL

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

Article 41 of the CSL recognises **consent** as a legal basis to process personal information.

Similarities with the Specification

Under the GDPR, the **legal bases for the processing of personal data** are:

- **consent** given by the data subject for one or more specific purposes;
- where necessary for the **performance of a contract** to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- where necessary for c**ompliance with a legal obligation** to which the controller is subject; and
- where necessary in order to **protect the vital interests** of the data subject or of another natural person.

Under the Specification, consent is the main vehicle serving as a legal basis for the processing of personal information. As such, any other legal basis for the processing of personal information is an exception to the need to obtain consent. Altogether, under Articles 5.4 and 5.6 of the Specification the recommended legal bases for the processing of personal are:

- **consent** given by the personal information subject or its guardian when the personal information subject is a child;
- where necessary for the **execution and performance of a contract** required by the personal information subject;
- where necessary for **compliance with a legal obligation** to which the personal information controller is subject;
- where necessary in order to **protect the vital interests** of the personal information subject or another natural person, **however, only when consent or authorisation from the natural person is difficult to obtain**.

GDPR	CSL Specification

Differences with the CSL

Under the GDPR, there are **multiple legal bases** for processing personal data (as described above).	The CSL states that network operators must obtain consent of the users whose data is being collected, but **does not outline alternative legal grounds**.
The GDPR includes **specific information** on how consent must be obtained and can be withdrawn.	The CSL **does not** explicitly provide information on how consent must be obtained and can be withdrawn.
Under the GDPR, as a general rule, the processing of **special categories of personal data is restricted unless** an exemption applies, which include the data subject's **explicit consent**.	The CSL **does not** contain explicit provisions on the processing of special categories of personal information.

Differences with the Specification

Under the GDPR, the legal bases for the processing of personal data also include • where necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller; and • the **legitimate interest** of the data controller where necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. The processing of personal data strictly necessary for the **purposes of preventing fraud** also constitutes a legitimate interest of the data controller concerned. The processing of personal data for **direct marketing purposes** may be regarded as carried out for a legitimate interest.	Under Article 5.6 of the Specification other recommended legal bases for the processing of personal information as an exemption from consent are: • where the processing is directly related to **national security and national defence security**; • where the processing is directly related **to public safety, public health, and major public interests**; • where the processing is **directly related to criminal investigation, prosecution, trials, or the execution of a judgment**; • where **the personal information involved** in the processing **has been made public by the personal information subject**; • when **collecting personal information from legally disclosed information**, such as legal news report, government information disclosure and other channels; • **where necessary for maintaining the safe and stable operation of a product or service**, such as finding and disposing of the faults in a product or service; and • **where the personal information controller is a news unit and that the processing is necessary for legal news reporting**.
Under the GDPR, there are specific legal bases for the processing of **sensitive personal data**.	The Specification **does not** contain specific legal bases for the processing of personal sensitive information.

4. Controller and processor obligations

4.1. Data transfers

Both the GDPR and the CSL provide for the transfer of personal data/information to third countries or international organisations. The GDPR and the CSL differ, though, on the regulation of such transfers, and the CSL provides data localisation requirements which the GDPR does not. Unlike the CSL, the GDPR recognises the concept of adequacy, and stipulates multiple legal grounds for international transfers of data.

The Specification does not provide specific requirements for cross-border transfers of personal information.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR Articles 13, 44-50 Recitals 101, 112	CSL Article 37 Specification Article 9.8, Annex D
Similarities with the CSL	
Not applicable.	Not applicable.
Similarities with the Specification	
Under the GDPR, **data subjects must be informed of the controller's intention to transfer personal data to a third country or international organisation** and the existence or absence of an adequacy decision by the European Commission, or where applicable, reference to appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.	Under Annex D.1 of the Specification, it is recommended that the cross-border transfer of personal information **should be separately listed or highlighted** in the privacy notice.
Differences with the CSL	
In the absence of a decision on an adequate level of protection, a transfer is permitted when **the data controller or data processor provides appropriate safeguards** with effective legal remedies that ensure the data subjects' rights as prescribed under the GDPR. **Appropriate safeguards include**: • binding corporate rules ('BCRs') with specific requirements (e.g. a legal basis for processing, a retention period, complaint procedures, etc.);	The CSL **does not** contain any concept of appropriate safeguards applicable to cross-border transfers such as SCCs, BCRs, approved codes of conduct, etc.

Differences with the CSL (cont'd)

- standard data protection clauses ('SCCs') adopted by the European Commission or by a supervisory authority;
- an approved code of conduct; or
- an approved certification mechanism.

The GDPR allows personal data to be transferred to a third country or international organisation that has an **adequate level of protection** as determined by the EU Commission.

The CSL **does not** establish that cross-border transfers may be allowed where based on an adequacy decision. However, under Article 37 of the CSL, 'if, due to business requirements, it is necessary [for operators of CII] to provide such information/data outside of the territory of Mainland China, **a security assessment shall be conducted** according to the measures jointly formulated by the national cyberspace authorities and relevant departments of the State Council.'

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

The CSL **does not** specify that a cross-border transfer is allowed based on international agreements for judicial cooperation.

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

The CSL **does not** outline similar grounds for a cross-border transfer.

One of the following **legal bases** can be applied to the transfer of personal data abroad:

- prior **consent**;
- when a data subject has explicitly **consented** to the proposed transfer and acknowledged the possible risks of such transfer due to inadequate safeguards;
- when the transfer is necessary for the performance or conclusion of a **contract**;
- when the transfer is necessary for important **public interest** reasons;
- when the transfer is necessary for the establishment, exercise, or defence of a **legal** claim; and
- when the transfer is necessary to protect the **vital interests** of a data subject or other persons.

The CSL **does not** provide similar legal grounds for a cross-border transfer.

GDPR	CSL Specification

Differences with the CSL (cont'd)

The GDPR **does not** provide for any personal data localisation requirements.	Article 37 of the CSL, which provides **data localisation requirements**, states that 'operators of critical information infrastructure that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China shall store such information/data within Mainland China.'

Differences with the Specification

The GDPR **provides several legal grounds** for the international transfer of personal data (as described above).	Under Article 9.8 of the Specification, cross-border transfers of personal information **do not have any additional requirements** in relation to the requisite legal basis beyond that they should comply with relevant laws and regulations.

4.2. Data processing records

Unlike the CSL, the GDPR establishes a legal obligation for controllers and processors to maintain a record of the processing activities under their responsibility. The GDPR also details the information that needs to be recorded.

The Specification similarly recommends establishing a record of the personal information processing activities, albeit without a separation between controller and processor processing activities.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR Articles 30 Recitals 82	CSL Specification Article 6.2, 11.3
Similarities with the CSL	
Not applicable.	Not applicable.
Similarities with the Specification	
Under the GDPR, **controllers and processors must maintain a record** of their processing activities.	Under Article 11.3 of the Specification, **it is recommended that personal information controllers have in place a record of their personal information processing activities**.
The GDPR establishes that **data controllers must record**: • 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; and • **international transfers of personal data**.	Under Article 11.3 of the Specification, **personal information controllers should record**: • the **purpose** of the personal information processing; • **the type** of personal information processed; • **the information about entrusted parties, transfers**, sharing or disclosure of the personal information; and • **international transfers of personal information.**
Differences with the CSL	
The GDPR **provides several requirements related to controllers and processors maintaining records** (as described above and below).	The CSL **does not** contain provisions requiring network operators to maintain personal information processing records.

GDPR	CSL Specification
Differences with the Specification	
The GDPR establishes that **data controllers must record**: • the **name and contact details of the controller**; • a description of the **categories of data subjects**; • **the identification of third countries or international organisations** when the processing involves an international-transfer of personal information; • **the documentation of suitable safeguards** adopted for international transfers of personal data; • **the estimated time limits for erasure of the categories of data**; and • **a general description of the technical and organisational security measures adopted**.	The Specification **does not** contain such recommendations.
The GDPR **does not** contain such requirements.	Under Article 11.3 of the Specification, personal information controllers should also record: • **the quantity and source** of the personal information; and • **the information of the relevant organisations, personnel, and information systems** linked to the personal information processing.
Under the GDPR, **organisations employing fewer than 250 persons need not maintain such a record** unless 'the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.'	The Specification recommendation **does not contain a specific threshold** to adopt a record of the personal information processing activities.
The GDPR establishes that **data processors must record**: • the name and contact details of the processor; • the categories of processing conducted on behalf of each controller; • international transfers of personal data, with the identification of third countries or international organisations, and the documentation of adopted suitable safeguards; and of third countries or international organisations, and the documentation of adopted suitable safeguards; and • a general description of the technical and organisational security measures that have been adopted.	The Specification **does not distinguish between personal information controllers and entrusted parties** regarding the recommendation of implementing and maintaining a record of the personal information processing activities.

4.3. Data protection impact assessment

CSL
Inconsistent

Specification
Fairly inconsistent

The GDPR establishes the requirement for a Data Protection Impact Assessment ('DPIA') to be performed in order to assess the risk of data processing activities to the rights and freedoms of data subjects in specific circumstances. In addition, the GDPR specifies the cases where a DPIA is required. Comparatively, the CSL only provides for cybersecurity risk assessments that operators of CII are obliged to conduct.

The Specification also includes a personal information security impact assessment that has certain similarities with the GDPR's DPIA, although the Specification focuses on different elements and controls.

Please note that the CSL provides binding legal requirements, and the Specification only provides recommendations.

GDPR	CSL Article 37-39
Articles 35-36 Recitals 75, 84, 89-93	Specification Articles 3.9, 7.6, 7.7, 9.1, 9.2, 9.4, 10.4

Similarities with the CSL

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

Under Article 38 of the CSL, at least once per year, operators of CII **must conduct an assessment of potential network security risks**, either personally or by entrusting a cybersecurity services provider. Such assessment can include data protection, albeit it is understood to primarily focus on cybersecurity.

Similarities with the Specification

The GDPR **establishes the requirement for a DPIA** to be conducted in specific circumstances. Member State supervisory authorities can further determine which processing operations require a DPIA.

Article 10.4 of the Specification establishes the requirements for **a personal information security impact assessment** ('PISIA').

The GDPR states that a DPIA is 'an assessment of the **impact of the envisaged processing operations on the protection of personal data**.'

Article 3.9 of the Specification defines PISIA as '**the process to evaluate the risks of damage to the legitimate rights and interests of the personal information subjects in light of the personal information processing activities**, to check their legal compliance, and to assess the effectiveness of the measures to protect the personal information subject.'

The GDPR states that a DPIA is required **when a systematic and extensive evaluation** of personal aspects relating to natural persons is involved that **is based on automated processing**.

Under Article 7.7 of the Specification, it is recommended to perform a PISIA **when using information systems with automatic decision mechanisms**.

GDPR	CSL Specification

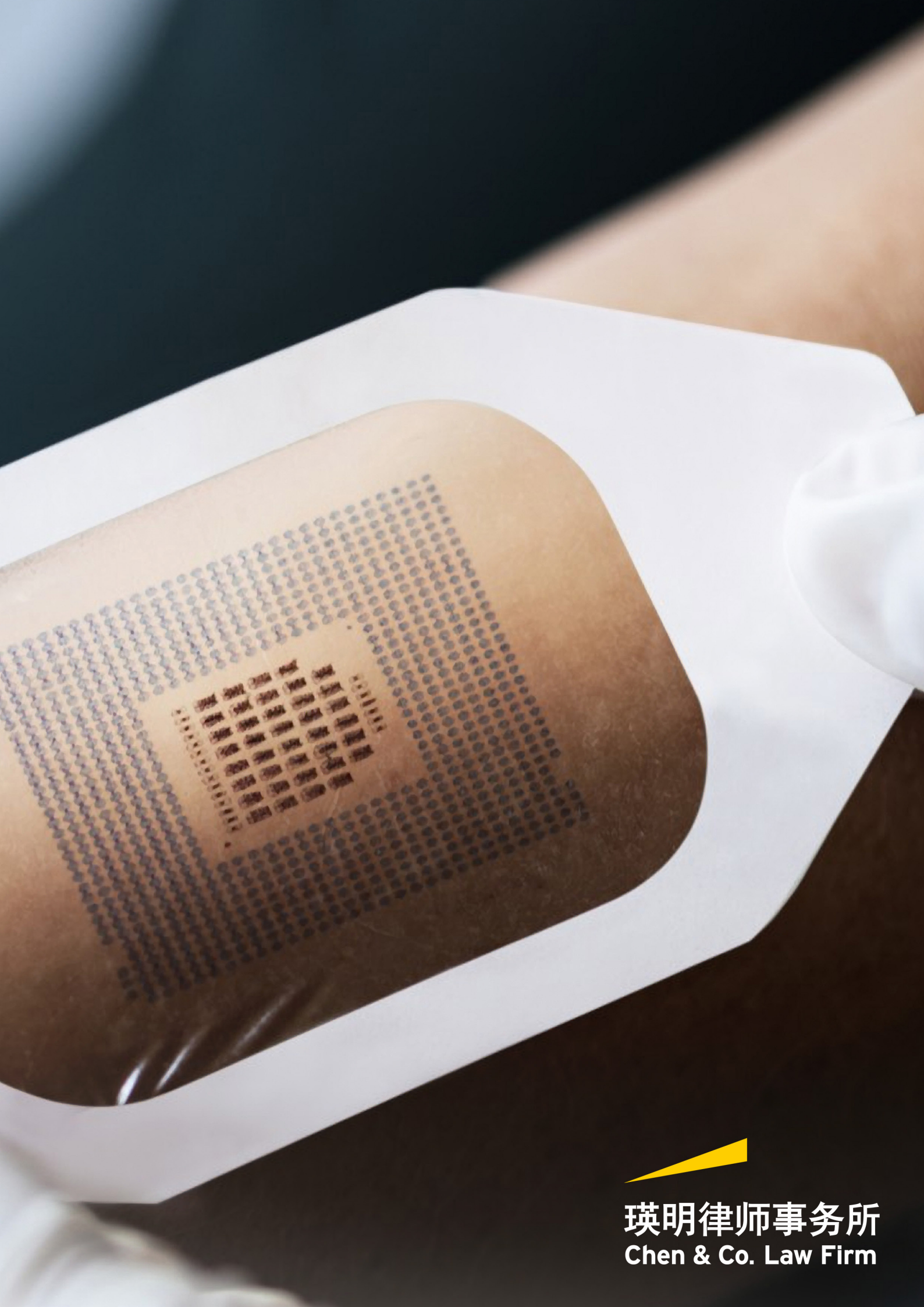
Similarities with the Specification (cont'd)

The GDPR states that a DPIA must include at least: • **an assessment of the necessity and proportionality** of the processing operations in relation to the purposes; • **an assessment of the risks to the rights and freedoms of data subjects**; and • **the measures contemplated for addressing the risks**, including safeguards, security measures, and mechanisms to ensure the protection of personal data and demonstrate compliance with the GDPR.	Article 10.4 of the Specification states that a PISIA should include at least: • whether the collection of personal information has been done following the **principles of clear purpose, consent, and necessity**; • whether the processing **can cause adverse effects on the legitimate rights and interests of the personal information subject**, including whether it will endanger personal and property safety, damage personal reputation and physical and mental health, as well as lead to discriminatory treatment; and • **the effectiveness of the security measures aimed at protecting the personal information**.

Differences with the CSL

The GDPR provides that **DPIAs should be conducted** when there is a change in security risks, new technologies are used, or there is high risk, automated, large scale, or systematic processing.	The CSL **does not** explicitly require risk assessments under such circumstances.
The GDPR **specifies** information that a DPIA should include.	The CSL **does not** detail the information that an assessment must contain.
A data controller **must consult** the supervisory authority prior to any processing that would result in a high risk in the absence of risk mitigation measures as indicated by the DPIA.	The CSL **does not** require consultation with supervisory authorities in relation to high risk processing. However, Article 38 of the CSL requires that the **results of annual security assessments and improvement measures should be submitted** to the relevant department responsible for the security of CII. Furthermore, under Article 39, the national cyberspace authorities or an entrusted cybersecurity service provider, may conduct random **testing and assessment of security risks**, and where necessary **propose measures for improvement**.
The GDPR **does not** specifically require DPIAs for data transfers by operators of CII.	Article 37 of the CSL provides that if, due to business requirements, it is necessary for operators of CII **to provide personal information outside of the territory of mainland China**, a security assessment shall be conducted.

GDPR	CSL Specification
Differences with the Specification	
The GDPR also states that a DPIA is required when: • the processing is likely to result in **a high risk to the rights and freedoms of natural persons**; • **processing on a large scale of special categories of data**; and • **having a systematic monitoring of a publicly accessible area on a large scale**.	Under Articles 7.6, 9.1, 9.2, and 9.4 of the Specification, it is also recommended to perform a PISIA: • **when aggregating and fusing personal information collected for different business purposes**; • **on the entrusted party when delegating processing of personal information**; • **when transferring personal information for reasons other than acquisition, merger, reorganisation, or bankruptcy**; and • **prior to publicly disclosing personal information when authorised by law or with reasonable reasons**.
The GDPR states that a DPIA must also include at least **a systematic description of the estimated processing operations and the purposes of the processing**.	Article 10.4 of the Specification states that a PISIA should also include at least: • when applicable, **the risk of re-identifying the personal information** after de-identification or anonymisation or when combining the collected information with other datasets; • **the possible adverse effects of the sharing, transferring, and public disclosure of personal information on the legitimate rights and interests of personal information subjects**; and • **if a security incident occurs, whether it would adversely affect the legitimate rights and interests of the personal information subject**.
Under the GDPR, where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk, **the controller must consult the supervisory authority** prior to processing.	The Specification **does not** provide such requirements for PISIAs.



瑛明律师事务所
Chen & Co. Law Firm

4.4. Data protection officer appointment

The GDPR provides for the appointment of a data protection officer ('DPO'), while the CSL does not contain a similar concept.

Although the Specification contains recommendations regarding a role similar to that of DPO, the Specification version of a DPO has significantly more discretion and powers in making decisions and implementing them.

Please note that the CSL contains legally binding requirements, and the Specification only contains recommendations.

GDPR Articles 13-14, 37-39 Recital 97	CSL Articles 21, 34 Specification Article 10.1

Similarities with the CSL

Not applicable.	Not applicable.

Similarities with the Specification

The GDPR provides for **the appointment of a DPO**.	Article 10.1 of the Specification provides for the **nomination of a person in charge of personal information protection**.
The GDPR requires that the appointed DPO must be designated on the basis of professional qualities and, in particular, **expert knowledge of data protection law and practices, and the ability to fulfil the tasks** referred to in Article 39.	Under Article 10.1(b) of the Specification, the appointed person in charge should have both the **relevant management work experience and professional knowledge experience for their role**.
The GDPR stipulates that the DPO must **directly report to the highest management level** of the controller or the processor.	Article 10.1(b) of the Specification states that the person in charge should **directly report to the person in charge of the organisation.**
The GDPR states that **the DPO must be provided with monetary and human resources** to fulfil their tasks.	Article 10.1(e) of the Specification states that **the person in charge should be provided with the necessary resources** to ensure their financial independence.

Differences with the CSL

Under the GDPR, data controllers and data processors, including their representatives, are required to **appoint** a DPO.	The CSL **does not** provide a requirement for network operators or operators of CII to appoint a DPO. Under Article 21, network operators are required to formulate internal security administration rules and operating procedures, **determine the persons in charge of cybersecurity**, and carry out their

GDPR	CSL Specification

Differences with the CSL (cont'd)

	cybersecurity responsibilities. In addition, under Article 34, operators of CII must **establish specialised security management institutions and persons responsible for security management**, and conduct security background checks on those responsible persons and personnel in critical positions. However, such a role would be focused on cybersecurity compliance
The GDPR **defines** the tasks of a DPO and conditions requiring a DPO, as well as, among other things, reporting processes, independence obligations, and qualifications related to DPOs (as described above and below).	The CSL **does not** contain similar provisions.

Differences with the Specification

The GDPR defines the tasks of a DPO, which include: • **inform and advise the controller or processor** of their obligations under the GDPR; • **monitor compliance** with data protection law and raise awareness/training the staff involved in processing operations; • provide **advice on DPIAs** when requested; and • act as the **point of contact for data subjects and supervisory authorities**.	Article 10.1(d) of the Specification provides that the responsibilities of the person in charge should include at least: • the **overall planning and implementation of personal information security** within the organisation, as well as taking **direct responsibility for personal information security**; • organising the redaction of personal information protection; • formulate, issue, implement, and regularly **update personal information protection policies** and relevant procedures; • **establish, maintain, and update the list of personal information** processed by the organisation (including the type, quantity, source, receiver, etc.) and the access authorisation scheme; • **conduct the PISIA**, put forward countermeasures and suggestions for personal information protection, as well as urging for security risks mitigation; • organise and carry out **personal information security training**; • **conduct an assessment before products and services are launched** to avoid unknown collection, use, sharing, and other processing of personal information; • **publish complaint, reporting medium, and other relevant information**, as well as timely processing of complaints and reports; • conduct a **safety audit**; • **maintain communication with supervision and management departments**; and • inform and **report on personal information protection and incidents**.

GDPR	CSL Specification
Differences with the Specification (cont'd)	
Under the GDPR, **both controllers and processors** are under the obligation to appoint a DPO in specific circumstances.	The Specification **does not** contain such provisions.
Under the GDPR, the obligations to appoint a DPO **only applies to controllers and processors whose core activities** consist either of processing operations which **require regular and systematic monitoring of data subjects on a large scale**, or processing on a **large scale of special categories of data** and personal data relating to **criminal convictions.**	Article 10.1(c) of the Specification recommends the appointment of a DPO if one of the following conditions is met: • **the main business involves personal information processing and the number of employees is over 200**; • **there is processing of more than one million persons or there is an expected processing of more than one million persons within 12 months**; or • **there is processing dealing with the personal sensitive information of more than 100,000 persons**.
The data controller and/or the data processor must **publish the contact details of the DPO** as part of their privacy notice and communicate these details to the supervisory authority.	The Specification **does not** contain such a provision.
A **group of undertakings may appoint a DPO** provided that the DPO is easily accessible from each establishment.	The Specification **does not** have such a provision.
The GDPR establishes the **independence of the DPO**.	The Specification **does not** have specific independence requirements for the DPO from other stakeholders.

4.5. Data security and data breaches

Any processing under the purview of the GDPR and the CSL is covered by an obligation of security for the entity in charge. In particular, the CSL has major sections on the security obligations pertaining to network operators.

Concerning the notification of data breaches, both the GDPR and the CSL include an obligation to notify the relevant authorities, as well as the impacted data/personal information subjects in certain circumstances. However, whilst the GDPR includes a set timeline for such notification, the CSL remains vague (please note that the Regulations of the People's Republic of China for Safety Protection of Computer Information Systems ('Safety Regulations') provides a clearer timeframe for reporting to the relevant authorities).

The Specification contains detailed information on security measures to be taken, including emergency response plans and the notification procedure for security incidents.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL Articles 21, 40, 42 Safety Regulations Article 14 Specification Articles 4(f), 10.1, 10.2, 11.5, 11.6
Articles 5, 24, 32-34 Recitals 74-77, 83-88	

Similarities with the CSL

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

Article 40 of the CSL provides that network operators must 'strictly **maintain the confidentiality** of any user information collected and establish a **comprehensive system for protecting** user information.'

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

Article 42 of the CSL states that network operators '**adopt technical and other necessary measures to ensure the security of personal information** they collect and to prevent personal information from being disclosed, damaged, or lost.'

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

Article 42 further stipulates that in the event of such disclosure, damage, or loss of personal information, remedial measures shall be promptly taken by the network operator and the **matter shall be reported to the competent department**.

GDPR	CSL Safety Regulations Specification

Similarities with the CSL

The controller must **notify** the **data subject** of a data breach without undue delay if the data breach is likely to result in a **high risk** to the rights and freedoms of natural persons.	Article 42 also provides that the network operator must **notify users** in a timely manner of disclosure, damage, or loss of personal information. The CSL does not specify whether notification of the breach is reliant on whether the breach would likely result in a high risk to the rights and freedoms of such users.
The GDPR provides a **list of technical and organisational measures** that data controllers and data processors must implement where appropriate, such as pseudonymisation, encryption, and the ability to restore availability of, and access to, personal data in a timely manner in the event of physical or technical incidents, to ensure integrity and confidentiality.	Article 21 of the CSL provides a **list of technical and organisational measures** that network operators must implement, such as formulating internal security administration rules and operating procedures, determining the persons in charge of cybersecurity, technical measures to prevent computer viruses, cyberattacks, network intrusions, and the adoption of measures including data classification, backup of important data, and data encryption.

Similarities with the Specification

The GDPR recognises **integrity and confidentiality as fundamental principles** of data protection by stating that personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate **technical or organisational measures**.	Article 4(f) of the Specification recognises the principle of **integrity and confidentiality as a basic principle** of personal information protection by recommending that personal information controllers should have security capabilities matching the security risks posed, and take sufficient **organisational and technical measures to protect the confidentiality, integrity, and availability of personal information**.
The GDPR states that **data controllers and data processors must adopt technical and organisational security measures** that ensure a level of security appropriate to the risk taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.	Article 11.5 of the Specification recommends that the **personal information controller should, in accordance with the requirements of relevant national standards, establish appropriate data security capabilities**, implement necessary management and technical measures, and prevent the leakage, damage, loss, and tampering of personal information.

GDPR	CSL Safety Regulations Specification

Similarities with the Specification (cont'd)

Under Article 33(5) of the GDPR, the controller **must document any personal data breaches**, including **the facts relating to the personal data breach, its effects, and the remedial action taken**.

Under Article 10.1(c)(1) of the Specification, the personal information controller **should record the details of the breach** with at least:

- **the persons involved**;
- **the time of the event**;
- **the location**;
- **the personal information and number of people involved in the event**;
- **the name of the system where the event occurred**;
- **the impact on other interconnected systems**; and
- **whether the law enforcement agencies or relevant departments have been contacted**.

Under Article 10.1(c)(2) of the Specification, the personal information controller should assess the possible impact of the incident and take necessary measures to control the situation and eliminate risks.

Under the GDPR, in case of a data breach, the data controller must **also notify the data subjects involved, without undue delay**, when the personal data breach is likely to result in a high risk.

Article 10.1(c)(4) of the Specification recommends that personal information subjects **be notified when the personal information breach can cause serious harm to their legitimate rights and interests**.

The notification must include as a minimum:

- **description of the nature of the breach including, where possible, the categories and the approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned**;
- **contact details of the DPO or other contact point**;
- **the likely consequences of the breach**; and
- **measures taken or proposed to be taken to mitigate** the possible adverse effects.

Article 10.2 of the Specification states that the notification to the personal information subject should include at least:

- **the content of the security incident**;
- **the contact information of the personnel in charge of personal information protection**;
- **the impact of the security incident**; and
- **suggestions on how to prevent and reduce risks independently as well as remedial measures for the personal information subjects**.

GDPR	CSL Safety Regulations Specification

Similarities with the Specification (cont'd)

The GDPR provides a **list of security measures** that the controller and processor may implement, which include: • the pseudonymisation and encryption of personal data; • measures that ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; and • measures that restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.	Article 11.5 of the Specification stipulates that the personal information controller should, in accordance with the requirements of relevant national standards, **establish appropriate data security capabilities, implement necessary management and technical measures, and prevent the leak, damage, loss, and tampering** of personal information.
The GDPR states that the controller and processor shall **take steps to ensure that any natural person** acting under the authority of the controller or the processor who has access to personal data **does not process them except on instructions from the controller**, unless he/she is required to do so by Union or Member State law.	Article 11.6(a) of the Specification recommends that the **personal information controller sign confidentiality agreements with relevant personnel engaged in personal information processing**.

Differences with the CSL

Under the GDPR, the obligation of data controllers to notify data subjects when the data breach is likely to result in a high risk to the rights and freedoms of natural persons, **is exempted in certain circumstances** such as where: • appropriate technical and organisational protective measures have been implemented; • any subsequent measures have been taken in order to ensure that the risks are no longer likely to materialise; or • it would involve disproportionate effort.	The CSL **does not** outline similar exemptions.
The GDPR **provides a list of information** that must be, at minimum, **included in the notification** of a personal data breach. For example, a notification must describe the nature of the breach, the approximate number of data subjects concerned, and the consequences of the breach.	The CSL **does not** provide a list of information to be included in the notification of a data breach.
The GDPR states that **data processors must notify** the data controller without **undue delay** after becoming aware of the personal data breach.	The CSL **does not** provide a similar requirement.

GDPR	CSL Safety Regulations Specification

Differences with the CSL (cont'd)

Under the GDPR, a personal data breach must be notified to the supervisory authority **without undue delay** and, where feasible, **no later than 72 hours** after having become aware of the breach.

The CSL does not provide a specific timeframe with regard to reporting a data breach. However, network operators are required to report a data breach to a competent authority in a **timely manner**, which can be understood to be **no later than 24 hours** under Article 14 of the Safety Regulations.

Differences with the Specification

Under the GDPR, in case of a data breach, the data controller must notify **the competent supervisory authority unless the personal data breach** is unlikely to result in a risk for the data subject.

Article 10.1(c)(3) of the Specification states that the personal information controller should **report in time according to the national network security emergency plan and other relevant provisions**.

The GDPR **sets a timeframe** to notify the competent national authority as 'without undue delay and, where feasible, not later than **72 hours** after having become aware of it.'

The Specification **does not** set a specific timeframe to notify the relevant authorities.

The GDPR **does not** have such provisions.

Article 10.1(a) of the Specification recommends that an **emergency plan** for personal information security incidents be formulated.

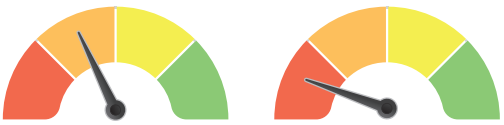
Article 10.1(b) of the Specification recommends that an **emergency response training and emergency drill be organised at least once a year** for relevant internal personnel to accustom them to their function and responsibilities, and to be informed of the emergency response strategies and procedures.

In addition, Article 10.1(d) of the Specification **recommends updating the emergency plan** in time according to the changes of relevant laws and regulations and the handling of incidents.

The notification must also include the **reason of any delay**.

Article 10.2 of the Specification states that the notification to the personal information subject should also include the **disposal measures taken or that will be taken**.

4.6. Accountability



CSL
Fairly inconsistent

Specification
Inconsistent

Both the GDPR and the CSL require that data controllers and network operators, respectively, take responsibility for certain concerns and demonstrate compliance.

Although the Specification does not directly recognise the principle of accountability, some of the underlying reasoning behind accountability is present.

Please note that the CSL provides binding legal requirements, and the Specification only provides recommendations.

GDPR Articles 5, 24-25 Recital 39	CSL Article 21 Specification Articles 4(e), 11.2, 11.7

Similarities with the CSL

The GDPR recognises **accountability** as a fundamental principle of data protection. Article 5 states that 'the data controller shall be responsible and able to demonstrate compliance with, paragraph 1 [accountability].' In addition, the principle of accountability can be taken to apply to several other obligations as mentioned in this Guide, including the appointment of a DPO and DPIAs.

The CSL does not explicitly refer to accountability as a fundamental principle. However, several provisions as referred to in other sections of this Guide can be taken as requiring that network operators **take responsibility and demonstrate compliance**, primarily with cybersecurity obligations, such as conducting risk assessments, carrying out cybersecurity responsibilities, and designating relevant staff.

Similarities with the Specification

The GDPR recognises **accountability** as a fundamental principle of data protection. Article 5 states that 'the controller shall be responsible and able to demonstrate compliance with data protection laws.'

Article 4(e) of the Specification recognises the principles of **openness and transparency**, stating that a 'personal information controller when processing personal information [...] should accept external supervision.'

Differences with the CSL

Not applicable.

Not applicable.

Similarities with the Specification

The GDPR clarifies that the data controller must implement measures that **ensure and demonstrate compliance**. It refers to **data protection by design and by default**, the implementation of data protection policies, and the **adherence to codes of conduct**. However, it does not specify which activities the data controller shall engage with.

Article 11.2 of the Specification recommends that when developing products or services with the function of processing personal information, the personal information controller **should consider personal information protection requirements during the phase of engineering the system**

GDPR	CSL Specification
Differences with the Specification (cont'd)	
	according to relevant national standards, and thus in order to ensure the simultaneous planning, construction and implementation of personal information protection measures during the development of the product or service.
The GDPR **does not** have such provisions.	Article 11.7 of the Specification recommends that personal information controllers have in place **audit processes to audit the effectiveness of personal information protection policies**, relevant procedures, and security measures.

5. Rights

5.1. Right to erasure

CSL
Fairly inconsistent

Specification
Fairly inconsistent

Both the GDPR and the CSL allow individuals to request the deletion of their personal information. However, under the CSL, the right to erasure is comparatively limited and the procedures for exercising such a right are not defined.

The Specification outlines recommendations that would provide a similar right to erasure as the GDPR, but the related mechanisms, circumstances, and exemptions differ.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL Article 43
Articles 12, 17, 23 Recitals 59, 65, 66	Specification Articles 5.5, 8.3, 8.7, 11.1

Similarities with the CSL

Under the GDPR, the data subject shall have the right to obtain from the controller the **erasure** of personal data concerning him/her without undue delay, and the controller shall have the obligation to erase personal data without undue delay in the event when the personal data have been **unlawfully processed.**

Under Article 43 of the CSL, if an individual discovers that a network operator has **violated the provisions of laws**, administrative regulations or user agreements in collecting or using an individual's personal information, he/she has the right to request the network operator to **delete** the personal information.

Similarities with the Specification

The GDPR provides individuals with the **right to request that their data be erased**.

Article 8.3 of the Specification provides personal information subjects with the **right to request that their personal information be erased**.

The scope of this right is not limited to the data controller, but **also impacts third parties**, such as recipients, data processors and sub-processors that may have to comply with erasure requests.

Article 8.3 of the Specification provides that the scope of this right should not be limited to the data controller, but **also impacts third parties**, such as recipients and data processors that may have to comply with erasure requests.

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

Article 8.7(c) of the Specification provides that this right of erasure should be exercised **free of charge**. There may be some instances, however, where a fee may be requested when the requests have a repetitive nature.

The data subject must be **informed** that they have the right to request for their data to be deleted.

Article 5.5(a)(5) of the Specification provides that personal information subjects should be **informed** that they

GDPR	CSL Specification

Similarities with the Specification (cont'd)

	have the right to request the erasure of their personal information, as well as the means to send such request.
Data subject requests under this right must be replied to without 'undue delay and in any event within **one month** from the receipt of the request.' The deadline can be extended to **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.	Article 8.7(a) of the Specification provides that personal information controllers should respond to personal information subject requests **within 30 days** or within the period specified by law.

Differences with the CSL

The right to erasure is viable if **certain grounds** apply, such as where **consent is withdrawn** and there is no other legal ground for processing, or **when personal data is no longer necessary for the purpose for which it was collected**.	The CSL **does not** contain equivalent provisions.
The GDPR **stipulates obligations** related to the right to erasure including mechanisms, timeframes, informing data subjects and controllers, and exemptions.	The CSL **does not** provide equivalent requirements.

Differences with the Specification

The right to erasure applies where: • the personal data are **no longer necessary in relation to the purposes for which it was collected or otherwise processed**; • **consent of the data subject is withdrawn** and there is with **no other legal ground** for processing, or the personal data **is no longer necessary** for the purpose of which it was collected; • there are **no overriding legitimate grounds** for processing; • the personal data has been erased for **compliance with a legal obligation** in EU or Member State law to which the controller is subject; or • the personal data has been collected in relation to the **offering of information society services**.	Article 8.3 of the Specification provides the right to erasure for personal information subjects **when one of the following conditions is met:** • when the personal information controller **collects and uses** personal information either in violation of laws and regulations, or in violation of the privacy notice agreed to by the personal information subject; • when the personal information controller **shares and transfers** personal information to a third party in violation of laws or regulations, or in violation of the privacy notice agreed to by the personal information subject; and • when the personal information controller **publicly discloses** the personal information in violation of the provisions of laws and regulations, or in violation of the privacy notice agreed to by the personal information subject.

GDPR	CSL Specification

Differences with the Specification (cont'd)

Methods to submit a request include **writing, verbally, and by other means, which include electronic means** when appropriate.	Personal information subjects should issue their request through the **means detailed in the privacy notice by the personal information controller** as the Specification does not explicitly open all means of communication to the personal information subject to issue a request.
The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is **made by the data subject** whose personal data is requested access to.	Article 11.1(d)(8) of the Specification provides that the personal information controller **may have a person in charge of personal information protection** that can process personal information subjects' request.
If the data controller has made personal data public and is obliged to erase the personal data, the data controller, taking into account the available technology and the cost of implementation, shall take reasonable steps, including **technical measures**, to **inform controllers** processing personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, such personal data.	The Specification **does not provide** an equivalent requirement.

5.2. Right to be informed

CSL
Fairly inconsistent

Specification
Fairly consistent

Both the GDPR and the CSL recognise the right to be informed as a tenet of data protection. Similarly, the Specification places the right to be informed at the centre of data protection. However, unlike the GDPR, the CSL does not address the right of data subjects to be informed regarding the existence of automated decision-making and profiling.

The Specification contains recommendations that are similar to the provisions of the GDPR in regard to transparency and providing information about processing to data subjects. The Specification and the GDPR differ, though, in several areas including in relation to informing data subjects individually, children's data, and legitimate interests.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL Article 41
Articles 5, 12-14, 23 Recitals 58-60	Specification Articles 4(e), 5.5, Annex D

Similarities with the CSL

Data subjects must be provided with information relating to the processing of personal data in order to validate their consent, including:

- **details of personal data** to be processed;
- **purposes** of processing, including the legal basis for processing;
- **data subject rights** (e.g. the right to erasure, right to object, right of withdrawal, right to lodge a complaint to a relevant authority, etc.);
- **data retention period**;
- **recipients or their categories** of personal data; and
- **contact details** of the data controller or its representative and the DPO.

A data controller cannot collect and process personal data for purposes other than the ones about which the data subjects were informed, **unless the data controller provides them with further information**.

Article 41 of the CSL establishes that to collect and use personal information, network operators shall disclose the processing of personal information and provide:

- the **rules of the processing collection and use**;
- the **purpose** of the processing; and
- the **means and scope** of the processing.

Article 22 of the CSL specifically applies to providers of network products and services, and requires that such providers indicate to users when they are collecting personal information and obtain user consent.

Article 41 of the CSL provides that network operators who collect and use personal information must disclose the rules for collecting and using such information, explicitly stating the **purposes, means, and scope for collecting or using information**, and obtain the consent of the users whose data is being collected.

GDPR	CSL Specification

Similarities with the Specification

The GDPR includes '**transparency**' as one of the **key principles** of data processing by affirming 'personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.'	Article 4(e) of the Specification recognises the principle of '**openness and transparency**' as a **fundamental principle** for personal information processing to be lawful, legitimate, and necessary.
The GDPR specifies that data subjects have the right to be provided with information about the processing of their personal data. In particular, they must have access to: • the **purposes** of the processing; • the **data retention period**; • the **categories of personal data, including special categories of data**; • the **data controller identity**; • the **recipients** (or their categories) of personal data; • the **data subjects' right**; • the **right to lodge a complaint with a supervisory authority**; • when data processing is based on a contract the **consequences of not providing the personal data**; and • the **transfer of data to third countries when applicable**.	Article 5.5(a) of the Specification recommends personal information controllers that provide personal information subjects with detailed information about personal information processing, which should include: • the **purposes of the processing**; • the **personal information retention period**; • the **types of personal information, including personal sensitive information**; • the **personal information controller identity**; • **the recipients of the personal information**; • the **personal information subjects' rights**; • the **right and the channels to lodge inquiries and complaints**, as well as **external dispute resolution agencies with their contact information**; • the **possible impact of not providing personal information**; and • the **transfer of personal information outside mainland China**.
The GDPR specifies that the information provided to the data subject must be given in a **concise, transparent, intelligible**, and **easily accessible** form.	Article 5.5(c) of the Specification recommends that information should be **clear and easy to understand** and conform to general language habits, the use of standardised numbers, diagrams, etc., and that **ambiguous language be avoided**.
For **consent** to be valid it must be **informed**.	Article 5.4(a) of the Specification stipulates that the personal information controller is **required to inform the personal information subject when collecting their consent**.
The GDPR specifies that the information provided to the data subject must be given in an **accessible form**.	Article 5.5(d) of the Specification recommends that the privacy policy be publicly published and **easy to access**.

GDPR	CSL Specification

Similarities with the Specification (cont'd)

The GDPR provides that where the controller intends to **further process personal data for a purpose other than that for which personal data was collected**, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information.

Article 5.5(f) of the Specification recommends that the personal information controller should amend the privacy notice **when matters described in the privacy notice change**, and that the personal information subject should be informed of such change.

Differences with the CSL

With regard to the right to be informed, the GDPR addresses **automated decision making, including profiling, possible consequences of a failure** to provide personal data, **how information can be provided** to data subjects, **examples of legitimate interest** circumstances, informing data subjects about **data transfers**, personal data that has been **collected from a third party, indirect collection**, and a **timeframe** for information to be provided to data subjects in relation to the processing of their personal data.

The CSL **does not** contain equivalent provisions.

Differences with the Specification

Under the GDPR, the following information needs to be included in the privacy notice:

- the **contact details of the DPO**; and
- the **existence of automated decision making**, including **profiling**, the **logic** involved, and the **consequences**.

Further information that should be included, as stated in Article 5.5 of the Specification, in the privacy notice is:

- the **possible security risks** of providing personal information; and
- the **basic security measures** taken to protect personal information.

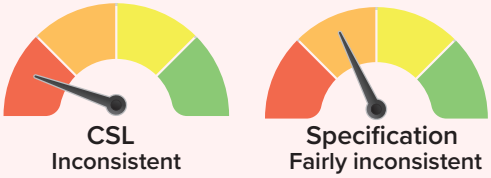
The GDPR **explicitly addresses the transparency obligations for indirect collection** of personal data.

Article 5.4(d) of the Specification **implicitly addresses transparency obligations** concerning the **indirect collection of personal data** by requiring personal information controllers involved in such collection to:

- require the personal information provider to explain the source of the personal information and confirm the legitimacy of the source;
- require the personal information controller to understand the scope of the authorisation and consent for the personal information processing obtained by the personal information provider; and

GDPR	CSL Specification
Differences with the Specification (cont'd)	
	• obtain the explicit consent of the personal information subject within a reasonable period after the personal information is collected where the processing activities go beyond the original scope of the authorised consent.
When the processing of personal data involves **children's personal data**, 'any information and communication [...] should be in such a clear and plain language that the child can easily understand.'	The Specification recommends treating **children's (under 14) personal information as personal sensitive information**, which, as per Article 5.5(a)(2) of the Specification, **should be clearly identified or highlighted in the privacy notice**. Furthermore, based on the sample privacy notice in Annex D of the Specification, it is recommended that a specific section on children's personal information collection be added. However, no specific language is recommended by the Specification.
When the processing is on the **legitimate interest** basis, the legitimate interest of the data controller and the third party must be specified in the privacy notice.	The Specification **does not** recognise legitimate interest as a valid ground for processing personal information.
The GDPR **only implies** that the information of the privacy notice should be true, accurate, and complete. The GDPR **does not** explicitly provide that data subjects should be informed one by one.	Article 5.5(b) of the Specification explicitly provides that the information of the privacy policy should be **true**, **accurate**, and **complete**. Article 5.5(e) of the Specification provides that **personal information subjects should be informed one by one**. But that when such information would prove to be too costly, the information can be made in the form of an announcement.

5.3. Right to object



Only the GDPR provides data subjects with the right to object and restrict the processing of their personal data, and to withdraw consent. In addition, the GDPR explicitly provides the right to opt out within the context of direct marketing. While this right to opt out is not present in the CSL, it is provided for in the Advertisement Law.

The Specification recommends that a right to withdraw consent and for processing to cease are provided, however, it does not outline exceptions to this right in the same manner as the GDPR.

Please note that the Advertisement Law and the CSL contain legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL
Articles 7, 18, 21, 23 Recitals 65, 70	Advertisement Law Article 43 Specification Articles 5.5, 8.3, 8.7

Similarities with the CSL and the Advertisement Law

The GDPR provides data subjects with the right to object to processing of their data for **direct marketing** purposes. In particular, in the context of direct marketing, opting out must be as easy as opting in.

The CSL does not provide equivalent provisions. However, Article 43 of the Advertisement Law provides that personal information subjects should be provided with **the means to refuse subsequent receipt of advertisements**.

Similarities with the Specification

Controllers shall no longer process personal data when requested by the data subject and in the circumstances listed in the law, including when **consent is withdrawn**.

Article 8.3(a) of the Specification stipulates that the personal information controller should no longer process personal information when requested by the personal information subject through the **withdrawal of consent**.

Information about data subject rights and on how to exercise them must be included in the privacy notice.

Article 5.5(a)(5) of the Specification stipulates that **information about the right to withdraw consent** and how to exercise it should be included in the privacy notice.

This right must be exercised **free of charge**.

Article 8.7(c) of the Specification provides that this right of withdrawal should be exercised **free of charge**. There may be some instances, however, where a fee may be requested when the requests have a repetitive nature.

Data subject requests under this right must be replied to without 'undue delay and in any event within **1 month** from the receipt of the request.' The deadline can be extended for up to **two additional months** taking into

Article 8.7(a) of the Specification provides that the personal information controller should respond to the personal information subject's request **within 30 days** or within the period specified by law.

GDPR	CSL Specification

Similarities with the Specification (cont'd)

account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.

The GDPR provides data subjects with the right to object to processing of their data for **direct marketing purposes**. In particular, in the context of direct marketing, opting out must be as easy as opting in.

Article 8.7(b) of the Specification specifically provides that the right to refuse further commercial advertisements based on their personal information must be guaranteed.

Differences with the CSL

The GDPR **provides for a right to object and to withdraw consent**. The GDPR also specifies that data subjects must be informed on **how to exercise** the right to object, a **timeframe for responses, circumstances where the right to object can be applied**, and **exceptions** that enable continued processing of data.

The CSL **does not establish** a right for natural persons to withdraw consent or object to processing. There is **no obligation for informing** natural persons or users on a right to object or withdraw consent in the CSL.

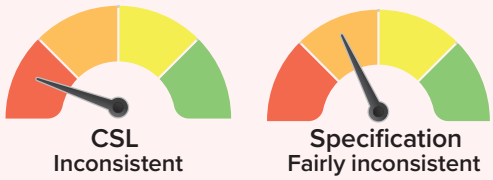
Differences with the Specification

Data subjects have the **right to the restriction of processing**:

- in order to contest the accuracy of the data;
- when the processing is unlawful;
- when the controller no longer needs the personal data but the data subject needs it for exercising legal claims or legal defence; or
- when the data subject has previously objected to the processing and the processing needs to be restricted in order to analyse the objection request.

The Specification **only covers** the right of withdrawal as a mechanism to restrict further processing of personal information and does not restrict this right.

5.4. Right of access



Unlike the GDPR, the CSL neither provides a right to access nor contains requirements for responding to requests for access.

The Specification recommends that personal information subjects have the right to access some of their personal information, however, this recommendation is more limited in scope than the right of access in the GDPR.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL
Articles 12, 15, 23 Recitals 59-64	Specification Articles 5.5, 8.1, 8.7, 11.1

Similarities with the CSL

Not applicable.

Not applicable.

Similarities with the Specification

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

Article 8.1 of the Specification recommends that personal information subjects have the **right to access** some of their personal information processed by the data controller.

The GDPR states that, when responding to an access request, a data controller must indicate:

- the **purposes** of the processing;
- the **recipients** or categories of recipient to whom the personal data have been or will be disclosed; and
- **any available information** as to their source when the data is not collected from the data subject.

Article 8.1 of the Specification provides that the personal information controller should respond to the personal information subject with:

- the **type of personal information** it holds about the personal information subject;
- the **source and purpose of the personal information**; and
- the **identity or type of third parties** which have obtained the personal information.

The GDPR provides that the right of access should not adversely affect the rights or freedoms of others, including trade secrets, **intellectual property**, and, in particular, **copyright protecting software**.

Article 8.7(e) of the Specification provides some exemptions to the right of access, such as:

- when the personal information is required for the **performance of legal obligations** by the personal information controller;
- when the personal information is **directly related to national security and national defence security matters**;
- when personal information is **directly related to public security, public health, and major public interests matters**;
- when the personal information is **directly related to criminal investigation, prosecution, trials, or the execution of judgments**;

GDPR	CSL Specification
Similarities with the Specification (cont'd)	
	• when the personal information controller has **sufficient evidence to demonstrate that the personal information subject is acting in bad faith or is abusing his/her rights**; • **in order to protect the life, properties, and other legitimate rights and interests of the personal information subjects or other persons where it is very difficult to obtain the consent of the relevant person**; • when responding to the request would **cause serious damage to the legitimate rights and interests of the personal information data subject or other individuals and entities**; and • when the request is **related to trade secrets**.
The GDPR states that data subjects can exercise this right **free of charge**. There **may be some instances where a fee may be requested**, notably when the requests are unfounded, excessive, or have a repetitive character.	Article 8.7(c) of the Specification provides that the right of access should be exercised **free of charge**. There may be some instances, however, where a fee may be requested when the requests have a repetitive nature.
Data subject requests under this right must be replied to without 'undue delay and in any event within **1 month** from the receipt of the request.' The deadline can be extended to **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.	Article 8.7(a) of the Specification provides that personal information controllers should respond to personal information subject requests **within 30 days** or within the period specified by law.
Data controllers can **refuse to act** on a request when it is **manifestly unfounded, excessive**, or has a **repetitive** character.	Article 8.7(e)(5) of the Specification personal information controller can **refuse an access request** when it has sufficient evidence that the personal information subject has **subjective malice** or is **abusing their rights**.
The data subject must be **informed** that they have the right to access their data.	Article 5.5(a)(5) of the Specification provides that the personal information subjects should be **informed** that they have the right to request access to their personal information, as well as the means to send such request.

GDPR	CSL Specification

Differences with the CSL

The GDPR **provides for the right to access**, that the exercise of such right **should not adversely affect the rights of others, and details information to be provided in a response** to a right to access request.	The CSL **does not** explicitly recognise the right to access, or provide similar requirements relating to such a right.

Differences with the Specification

Data subjects must have a variety of means through which they can make their request, including through **electronic means or verbally**.	Personal information subjects should issue their request through the **means detailed in the privacy notice by the personal information controller** as the Specification does not explicitly open all means of communication to the personal information subject to issue an access request.
When the access request is made through electronic means, the data controller should **submit the response through the same means.**	There is **no requirement** in the Specification that electronic requests should be responded to using the same means.
The GDPR states that, when responding to an access request, **a data controller must indicate**: • the **categories of personal data concerned**; • the r**etention period**; • the **right to lodge a complaint with the supervisory authority**; • the **existence of automated decision making**; and • the **existence of data transfers**.	The Specification only explicitly recommends personal information controllers to provide: • the **type of personal information** it holds about the personal information subject; • the **source and purpose of the personal information**; and • the **identity or type of third parties** which have obtained the personal information.
The GDPR specifies that data controllers must have in place **mechanisms** to ensure that the request is **made by the data subject** to whom the personal data that is the subject of an access request relates.	Article 11.1(d)(8) of the Specification provides that the personal information controller **should have a nominated person to assist** in processing personal information subject requests.

5.5. Right not to be subject to discrimination

The right not to be subject to discrimination in exercising rights is not mentioned in the CSL, and whilst it is not explicitly mentioned in the GDPR, it can be inferred from the fundamental rights of data subjects provided for in the GDPR.

The GDPR also recognises a right for data subjects to object to automated processing. The Specification similarly recommends providing a right to object to automated processing to the personal information subject, but in a more limited fashion than the GDPR.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL
Articles 5, 22, 23 Recitals 39, 71-73	Specification Article 8.5

Similarities with the CSL

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

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

Similarities with the Specification

The GDPR **protects individuals from automated processing** that may result in a decision with legal or significant effects, and that may have discriminatory consequences on the individuals by giving individuals the opportunity to challenge the decision and to ask for human intervention.

The GDPR protects individuals by, among other things, **limiting the legal basis upon which automated processing activity** may be carried out. The GDPR requires that **a data protection impact assessment be carried out where there is a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing**, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.

Article 8.5(c) of the Specification **recommends protecting personal information subjects from automated processing** that may have a significant impact on the rights and interests of the personal information subject by giving them the opportunity to challenge the decision and to ask for human intervention.

Article 8.5(a) of the Specification protects personal information by requiring that the personal information controller **perform an information security impact assessment at the planning and design stage or before the first use of automated processing**, adopt the results of the assessment, and take effective measures to protect the personal information subject.

GDPR	CSL Specification

Differences with the CSL

The **right not to be subject to discrimination** in exercising rights can be inferred from the fundamental rights of data subjects. The GDPR protects individuals from automated processing that may result in a decision with legal or significant effects.

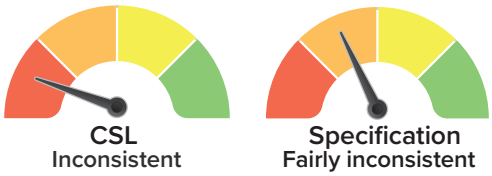
The right not to be subject to discrimination in exercising rights and automated processing of personal data is **not mentioned** in the CSL.

Differences with the Specification

The GDPR **does not** require that impact assessments related to automated processing be carried out at least once a year.

Article 8.5(b) of the Specification protects personal information by requiring **the personal information controller to carry out regular (at least once a year) personal information security impact assessments when using automated processing**, and to improve the measures to protect the personal information as per the result of the assessment.

5.6. Right to data portability



Unlike the GDPR, the CSL does not provide individuals with the right to data portability.

The Specification recommends that a right to portability should be provided, however, it restricts this right to three categories of personal information: basic data and identity information, personal health information, and personal education information.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL
Articles 12, 20, 23 Recital 68	Specification Articles 8.6, 8.7

Similarities with the CSL

GDPR	CSL
Not applicable.	Not applicable.

Similarities with the Specification

GDPR	CSL
The GDPR provides individuals with the **right to data portability**.	Article 8.6 of the Specification recommends providing personal information subjects with the **right to data portability**.
The GDPR provides that **individuals can request the data controller to have their personal data transmitted directly from one controller to another** where technically feasible.	Article 8.6 of the Specification provides that **individuals can request the direct transfer of the personal data covered by the right to portability to a third party designated by the personal information subject**, where technically feasible.
Anonymous data is **not** subject to the GDPR and therefore its portability is not subject to the restrictions attached to the right to data portability.	**Anonymous personal information** is not subject to the Specification, and therefore to personal information subject rights.
The GDPR provides that the right of access should not adversely affect the rights or freedoms of others, including trade secrets, **intellectual property**, and, in particular, **copyright protecting software**.	Article 8.7 of the Specification provides some exemptions to the right of portability, such as: • when the personal information is required for the **performance of legal obligations** by the personal information controller; • when the personal information is **directly related to national security** and **national defence security matters**; • when personal information is **directly related to public security, public health**, and **major public interests matters**; • when the personal information is **directly related to criminal investigation, prosecution, trials, or execution of judgments**;

GDPR	CSL Specification

Similarities with the Specification (cont'd)

	• when the personal information controller has **sufficient evidence to demonstrate that the personal information subject is acting in bad faith or is abusing their rights**; • **in order to protect the life, properties, and other legitimate rights and interests of the personal information subjects or other persons while it is very difficult to obtain the consent of the relevant person**; • when responding to the request would **cause serious damage to the legitimate rights and interests of the personal information data subject or other individuals and entities**; and • when the request is **related to trade secrets**.
The data subject must be **informed** that they have the right to data portability.	Article 5.5(a)(5) of the Specification provides that personal information subjects should be **informed** that they have the right to request that their personal information is transferred, as well as the means to send such request.
The GDPR states that data subjects can exercise this right **free of charge**. There **may be some instances where a fee may be requested**, notably when the requests are unfounded, excessive, or have a repetitive character.	Article 8.7(c) of the Specification provides that the right to data portability should be exercised **free of charge**. There may be some instances, however, where a fee may be requested when the requests have a repetitive nature.
Data subject requests under this right must be replied to without 'undue delay and in any event within **1 month** from the receipt of the request.' The deadline can be extended to **two additional months** taking into account the complexity and number of requests. In any case, the data subject must be informed of such extension within one month from the receipt of the request.	Article 8.7(a) of the Specification provides that personal information controllers should respond to personal information subject requests **within 30 days** or within the period specified by law.

Differences with the CSL

The GDPR provides individuals with the **right to data portability**, and defines the right to data portability as the **right to receive data processed on the basis of a contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format'** and to transmit that data to another controller without hindrance.	The CSL **does not** provide individuals with the right to data portability.

GDPR	CSL Specification

Differences with the Specification

The GDPR defines the **right to data portability as the right to receive data processed on the basis of a contract or consent and processed by automated means, in a 'structured, commonly used, and machine-readable format'** and to transmit that data to another controller without hindrance.	Article 8.6 of the Specification defines the right to data portability **as the right of a personal information subject to request copies of three types of personal information to be transferred to a designated third party of their choice**.
Article 20(3) of the GDPR explicitly states that **the right to data portability can be invoked while requesting the data controller to erase the personal data.**	The Specification **makes no mention** of allowing personal information subjects to invoke both the right to erasure and the right to data portability at the same time.
The GDPR **does not** explicitly limit the scope of the right to data portability to certain categories of personal data.	Article 8.6 of the Specification limits the right to data portability to **three categories** of personal information: • basic data and identity information; • personal health information; and • personal education information.

6. Enforcement

6.1. Monetary penalties

Both the GDPR and the CSL provide for the possibility of monetary penalties to be issued in cases of non-compliance. However, the nature of the penalties, the amount, and who is subject to them, differ. Furthermore, the CSL also provides for the sanction of directly responsible persons as well as sanctions beyond monetary penalties.

As a recommended standard, the Specification does not provide enforcement mechanisms for non-compliance. Sanctions may only be applied in relation to the Specification where a law or regulation requires compliance with the Specification.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR Article 83 Recitals 148-149	CSL Articles 59-69, 73 Specification

Similarities with the CSL

The GDPR provides for the possibility of administrative **monetary penalties to be issued** by supervisory authorities in cases of non-compliance.

Articles 59-69 of the CSL provide for the possibility of **monetary penalties to be issued** by supervisory bodies.

Similarities with the Specification

Not applicable.

Not applicable.

Differences with the CSL

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

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

The CSL **does not** specify comparable aspects to be considered when applying monetary penalties.

GDPR	CSL Specification

Differences with the CSL (cont'd)

• adherence to approved codes of conduct or approved certification mechanisms; and • any other aggravating or mitigating factor applicable to the circumstances of the case.	
Supervisory authorities may **develop guidelines** that establish further criteria to calculate the amount of monetary penalties.	The CSL **does not** explicitly provide that supervisory authorities may establish further criteria in order to calculate the amount of monetary penalties.
Depending on the violation occurred the penalty may be up to either: • **2% of global annual turnover or €10 million**, whichever is higher; or • **4% of global annual turnover or €20 million**, whichever is higher.	Under Articles 59-69 of the CSL, monetary penalties for network operators may range from: **RMB 10,000 (approx. €1,300)** to **RMB 1 million (approx. €130,000)** depending on the violation. In addition, fines of between **1 to 10 times the amount of any unlawful gains** may be imposed for certain violations.
Under the GDPR, it is left to EU Member States to **create rules** on the application of administrative **fines to public authorities and bodies.**	The CSL **does not provide** for additional rules to be applied to fines for public authorities and bodies.
Under the GDPR administrative fines may be applied to **government bodies**.	Article 73 of the CSL provides that the **personnel of government bodies** that use personal information for purposes other than obligations stipulated in the CSL, will be punished in accordance with the law.
The GDPR **does not** provide that fines may be imposed on directly responsible supervisors and personnel.	Articles 59-69 of the CSL provide that fines, which range from RMB 5,000 (approx. €650) to RMB 1 million (approx. €130,000) depending on the violation, may be applied to **directly responsible supervisors and personnel**.
The GDPR **does not** provide for data localisation requirements.	Article 66 of the CSL provides specific **penalties for operators of CII that fail to comply with Article 37 of the CSL on storing certain data in mainland China**, including fines of between RMB 50,000 (approx. €6,500) to RMB 100,000 (approx. €13,000) for operators, and between RMB 10,000 (approx. €1,300) to RMB 100,000 (approx. €13,000) for directly responsible personnel.

GDPR	CSL Specification

Differences with the Specification

The GDPR provides for **the possibility of administrative, monetary penalties** to be issued by the supervisory authorities in cases of non-compliance.

As a recommended standard the Specification **does not have enforcement mechanisms**. Non-compliance with the Specification would lead to sanctions only when a law or regulation requires compliance with the Specification.

6.2. Supervisory Authority

The GDPR provides for the establishment of a supervisory authority with corrective as well as investigative powers. The CSL reaffirms the authority of multiple relevant government bodies to exercise corrective and investigative powers, as well as the capacity to enact administrative regulations in order to strengthen data protection measures under their regulatory scope, as provided for elsewhere in PRC legislation.

While both the GDPR and the CSL provide authorities with the ability to handle complaints as well as subjecting them to potential review and sanctions in accordance with the law, there remain differences between the provisions regarding supervisory authorities. For instance, the CSL provides some additional obligations in relation to cybersecurity products, certifications, and the security of CII. Additionally, the CSL does not entrust one supervisory authority with regulatory powers over data protection matters, but multiple authorities. The Specification does not refer to authorities or the supervision of processing activities.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL Articles 14, 19, 23, 35, 39, 64, 73 Specification Article 1
Articles 51-84 Recitals 117-140	

Similarities with the CSL

Under the GDPR, supervisory authorities have **corrective powers** which include:

- **issuing warnings** and reprimands;
- imposing a temporary or definitive limitation including a **ban on processing**;
- ordering the **rectification or erasure of personal data;** and
- imposing administrative **fines**.

Under Article 64 of the CSL, the relevant authority and departments have the power to order network operators to take **corrective action** and **issue a warning**. If the network operator refuses to undertake corrective action, the relevant authority has the power to **issue a fine**. Additionally, the relevant authority or department has the power to require removal measures such as **deletion**, as well as to **notify the network operator** to block the transmission of prohibited information, **temporarily suspend operations, take down its website**, or revoke its business **permits or licences.**

Under the GDPR, supervisory authorities shall:

- handle complaints lodged by data subjects; and
- cooperate with data protection authorities from other countries.

Under Article 14 of the CSL, the relevant authority and departments shall:

- **handle reports or complaints** lodged by individuals and network operators;
- **transfer** complaints to **other authorities or departments** if the matter does not fall within its responsibility; and
- promote **information sharing** amongst authorities and departments, operators of CII, relevant research institutions, and cybersecurity service providers.

The GDPR outlines that supervisory authorities may be subject to **control or monitoring mechanisms** regarding their financial expenditure and to **judicial review**.

Article 73 of the CSL outlines that relevant authorities and departments may be subject to **sanctions in accordance with the law** for using acquired information beyond what is exclusively needed for cybersecurity protection.

GDPR	CSL Specification

Similarities with the CSL (cont'd)

Under the GDPR, supervisory authorities are tasked with **promoting public awareness** and understanding of the risks, rules, safeguards, and rights in relation to processing as well as promoting the **awareness of controllers and processors** of their obligations, amongst other tasks.	Under Article 19 of the CSL, relevant departments must organise and provide **regular publicity and education** on cybersecurity, and guide, supervise, and require relevant entities to provide such publicity and education on cybersecurity in an effective way. Furthermore, mass media must publicly provide education on cybersecurity to the society in a focused fashion.

Similarities with the Specification

Not applicable.	Not applicable.

Differences with the CSL

The GDPR **does not** cover the direct sanction of responsible individuals.	Under Article 64 of the CSL, the relevant authorities and departments have the power to impose a fine for data protection violations **on the persons directly in charge and other directly responsible persons**.
Under the GDPR, supervisory authorities have **investigatory powers** which include: • ordering a controller and processor to provide required information; • conducting data protection audits; • carrying out a review of certifications issued; and • obtaining access to all personal data and to any premises.	The CSL **does not** specify a list of the investigatory powers, which are to be formulated in other laws and regulations. However, the relevant authority shall be responsible for monitoring the security of online content. Under Article 14, they should also handle received reports on behaviours endangering cybersecurity or transfer such reports to the relevant department where applicable.
The GDPR **does not** include a similar provision in relation to a catalogue of equipment and products or certification and inspections.	Under Article 23 of the CSL, the national authorities together with the relevant departments of the State Council are tasked with **developing a catalogue** of critical network equipment and specialised cybersecurity products, and **publishing security certification and security inspection results** to avoid repeated certifications and inspections.
The GDPR **does not** include a similar provision in relation to measures for the protection and security of CII.	Article 39 of the CSL provides that the relevant authorities and departments should adopt the following **measures for protecting the security of CII**: • conducting security tests; • organising periodic cybersecurity drills; • promoting information sharing; and • providing technical support and assistance for cybersecurity response and recovery operations.

GDPR	CSL Specification

Differences with the CSL (cont'd)

The GDPR **does not** include a similar provision in relation to security reviews.	Article 35 of the CSL provides that the relevant authorities and departments should **conduct a security review** of operators of CII who purchase network products and services that may influence national security.
Supervisory authorities may be subject to **financial control** only if such control does not affect its independence. They have separate, public annual budgets, which may be part of the overall national budget.	The CSL **does not** contain a similar provision in relation to financial control.

Differences with the Specification

Under the GDPR, supervisory authorities have **investigatory and corrective powers** and are tasked with several responsibilities. There are also provisions relating to the determination of supervisory authorities by EU Member States.	Article 1 of the Specification only states that the Specification is applicable to the supervision, management, and evaluation of personal information processing activities by organisations such as competent regulatory authorities and third-party evaluation agencies. However, **no specific authority is mentioned, nor are their prerogatives regarding the supervision, management, and evaluation of personal information processing activities**.

6.3. Other remedies

CSL
Fairly consistent

Specification
Fairly consistent

In addition to administrative sanctions, any natural person has the right to seek compensation for any material and non-material damage resulting from a violation of the GDPR or the CSL. Only the GDPR, though, allows for both individual and collective action before the courts.

The GDPR specifies how damages are compensated by the controller and the processor. Neither the CSL nor the Specification address this point.

In addition to administrative sanctions and civil remedies, the CSL specifically refers to criminal sanctions when the violation of the CSL constitutes a crime under the Criminal Law of the PRC.

Please note that the CSL contains legally binding requirements, while the Specification only contains recommendations.

GDPR	CSL Articles 14, 43, 49, 74 Specification Articles 4(a), 9.2(g), 9.4(e)
Article 82 Recitals 146, 147	

Similarities with the CSL

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

Under Article 14 of the CSL 'any individual or organisation shall have the **right to report** conduct that endangers cybersecurity to the cyberspace authorities, telecommunications authorities, public security authorities, or other relevant authorities.'

Furthermore, Article 49 requires network operators to set up **complaint and reporting systems** for network information security, disclose the ways of complaint and reporting and other information, and promptly accept and handle complaints and reports related to network information security.

Similarities with the Specification

The GDPR provides individuals with a **cause of action to seek material or non-material damages** for violation of privacy laws before the courts.

Article 4(a) of the Specification stipulates that the personal information controller should bear the responsibility when personal information processing activities cause damage to the legitimate rights and interests of the personal information subjects.

Article 9.2(g) and 9.4(e) reiterate the **civil responsibility of the personal information controller when causing damage to the legitimate rights and interests of the personal information subjects** due to a security incident, transfer of personal information, or when publicly disclosing personal information.

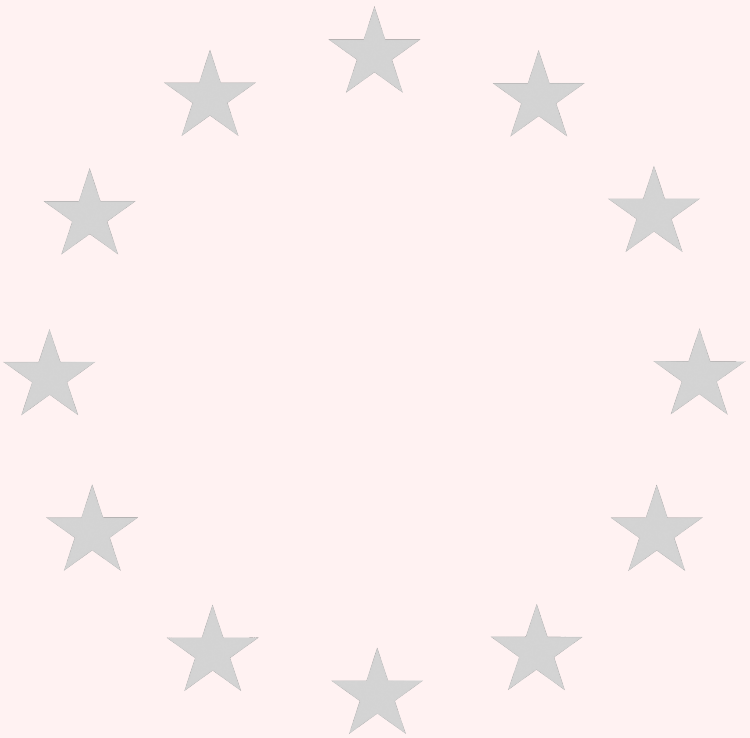
GDPR	CSL Specification

Differences with the CSL

The GDPR provides individuals with a cause of action to **seek compensation** from a data controller and data processor for a violation of the GDPR.	The CSL **does not** explicitly provide individuals with a cause of action to seek compensation from a network operator. However, **Article 74 recognises** that when a network operator violates the CSL, and in so doing causes damage to others, **civil liability shall be borne**. In such cases, individuals should be able to invoke the Tort Law of the PRC to seek compensation.
The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to a **not-for-profit body, association, or organisation** that has as its statutory objective the protection of data subject rights.	The CSL **does not** address this issue.
The GDPR provides that a data controller or processor shall be **exempt from liability to provide compensation** if it proves that it is not in any way responsible for the event giving rise to damage.	The CSL **does not** explicitly provide such exemptions.

Differences with the Specification

The GDPR allows Member States to provide for the possibility for data subjects to give a mandate for representation to a **not-for-profit body, association, or organisation** that has as its statutory objective the protection of data subject rights.	The Specification **does not** address this issue.
The GDPR **specifies how damages are compensated** by the controllers and processors responsible for the damage.	The Specification **does not** specify how damages are compensated by the personal information controllers responsible for the damage.

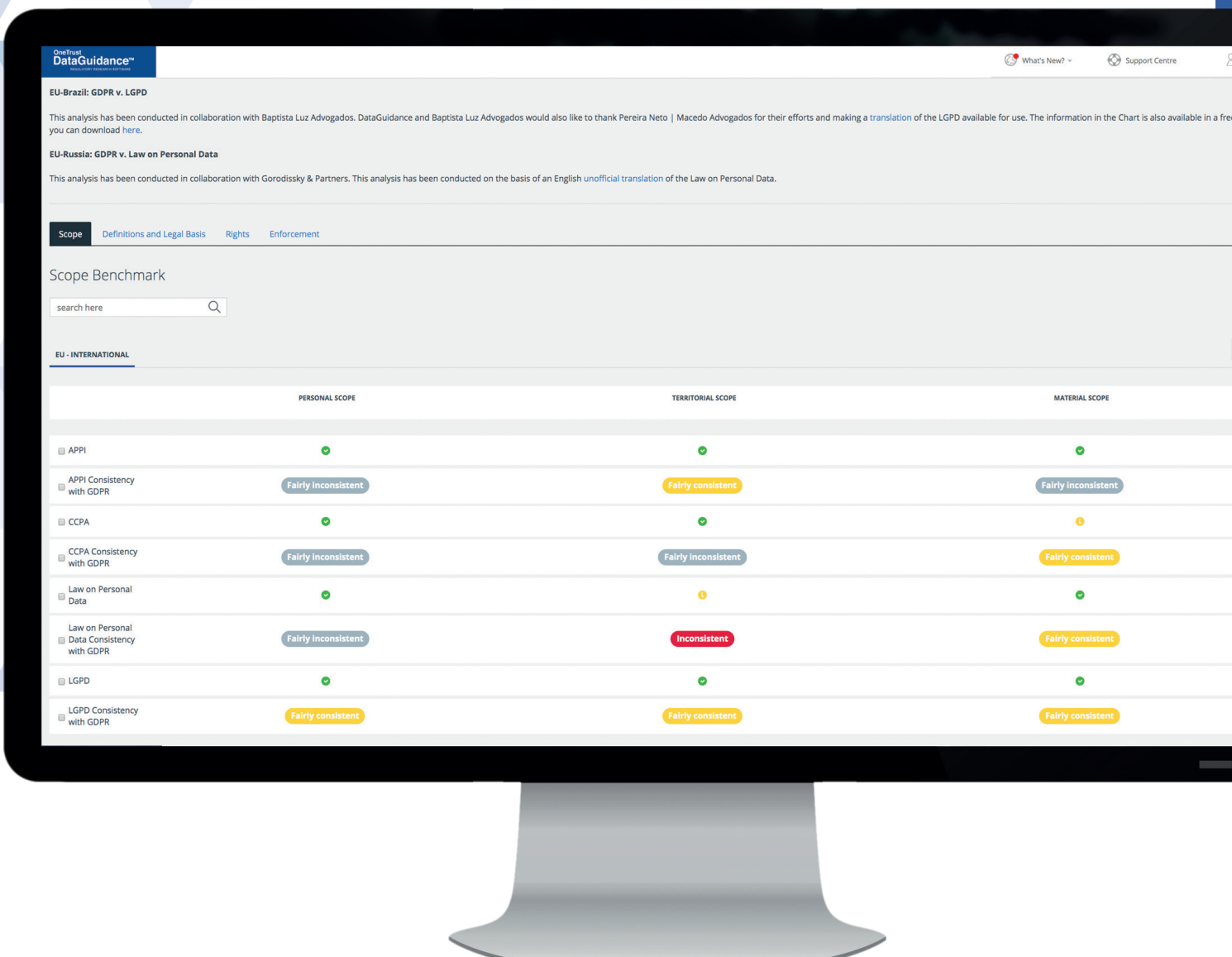


OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Global Regulatory Research Software

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

Monitor regulatory developments, mitigate risk
and achieve global compliance.



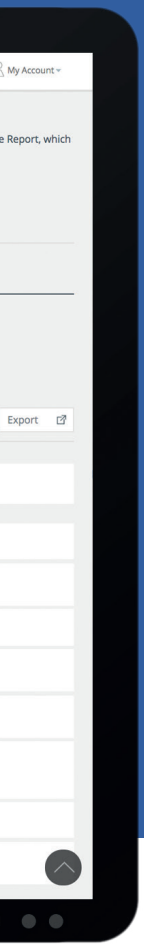
Build a global privacy program by comparing key legal frameworks against the GDPR

CCPA | Russia | Thailand | Brazil | Japan

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

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

- Scope
- Rights
- Definitions and legal basis
- Enforcement



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

Start your **free trial** today at **dataguidance.com**