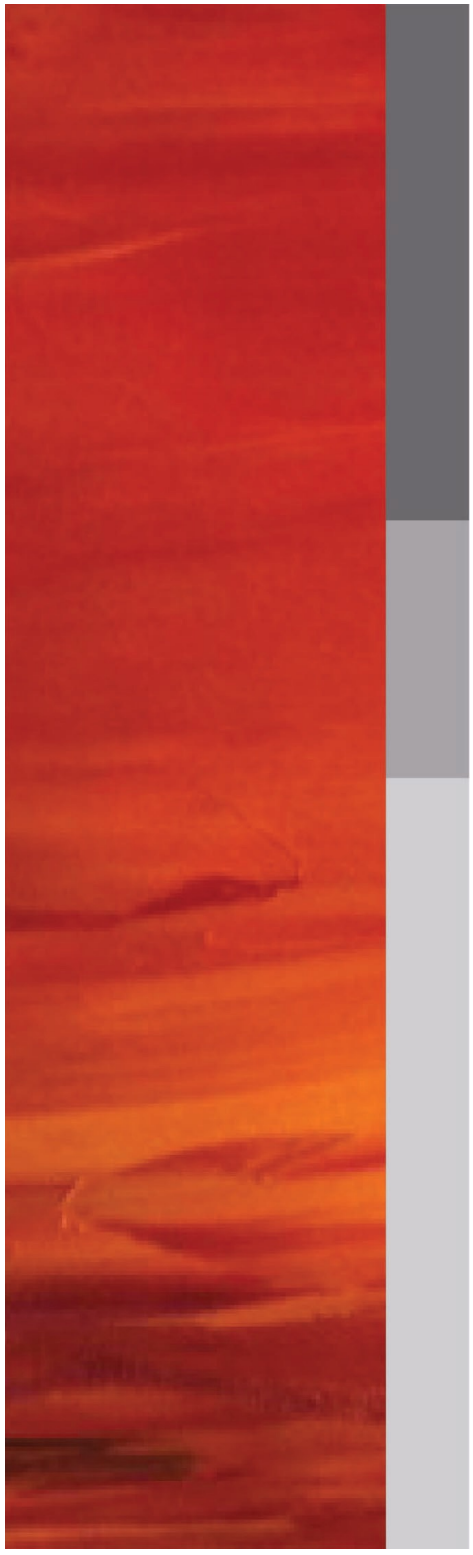


PERSONAL INFORMATION PROTECTION IN CHINA

ASIALLIANS

Avocat | Attrorneys-at-law
Réseau Asiallians | Asiallians Network

An topicality that is still uncertain, unstable, equivocal, imprecise, hesitant, floating, indecisive, insecure.

Article 38 of PIPL / cross-border data transfers (“CBDT”)

Beijing
Until Feb 22, 2023
48 Application has been filed
(142 enterprises reached Beijing CAC to express that they are willing to file the application, many of which are still preparing the application)
2 Approval issued by CAC

Shanghai
Untill Feb 1, 2023
67 Application has been filed
0 Approval issued by CAC

Chinese new year 2023 (1 month before deadline…)
Name of the certification organization: 中国网络安全审查技术与认证中心
(China Cybersecurity Review Technology and Certification Center)
Telephone: 010-82261100
Link: https://data.isccc.gov.cn/#/pip/login

ASIALLIANS

BACKGROUND AND LEGAL FRAMEWORK

The digital economy has become a substantial key driver of development and growth in China and represents essential parts of the daily lives of Chinese citizens and companies. Chinese tech giants have become international champions, launching products/services in China and on overseas markets, listing on foreign stock exchanges – procedures which have occasionally involved data misuse and privacy violations.

China has significantly strengthened its governance system for cybersecurity, data and personal information protection.

The cornerstone of these efforts has been the country's concept of cyber sovereignty: embedded in the **2015 National Security Law**, it represents a model of governance where the Chinese state has the ultimate authority in the cyberspace, within its boundaries but also on international activities affecting its national security, public interests and rights of its citizens and organisations.

BACKGROUND AND LEGAL FRAMEWORK

Cybersecurity Law (CSL), - June 2017 - is the first omnibus law governing cybersecurity and information protection, enshrining the concept of cyber sovereignty in its first article, and outlining obligations for network operators, internet service providers, platform operators, digital products and services, and critical information infrastructure operators.

Data Security Law (DSL), - September 2021 - outlines a comprehensive data classification and security system to govern data creation, collection, storage, processing, and transfer, both within China and outside China when potentially affecting China's national security or public interest. The DSL clarifies the distinction among (i) core data; (ii) important data; and (iii) generic data.

Personal Information Protection Law (PIPL), which - November 2021 - defines the rights of personal information owners in China and stipulates obligations for personal information processors, including for storage and cross-border transfers outside of China.

BACKGROUND AND LEGAL FRAMEWORK

At the same time, various regulations and departmental rules have been enacted to support the implementation and enforcement of the three laws.

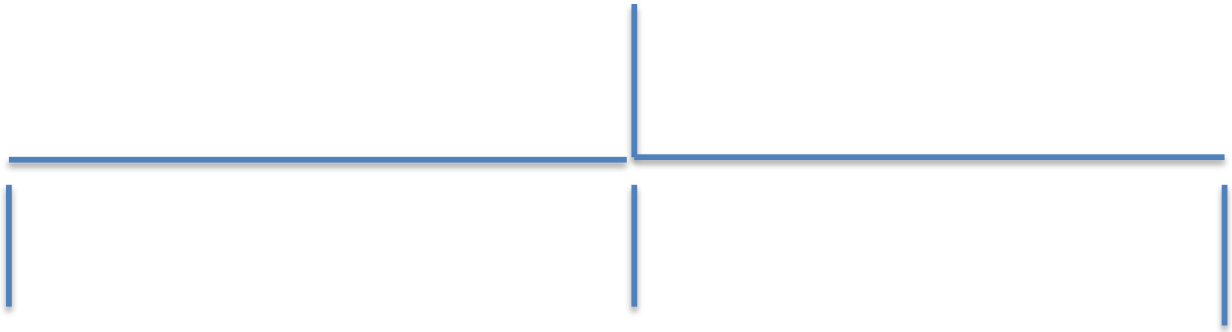
Although the more concerned parties are Chinese tech giants, any company operating within the territory of China – including foreign ones – are affected.

So are foreign companies based abroad providing products or services to Chinese companies or citizens.

Moreover, relevant industry associations and key domestic companies have driven the formulation of numerous technical standards and specifications to further supplement existing regulations and rules – some of which are increasingly being pushed globally to promote the internationalisation of China's governance model.

BACKGROUND AND LEGAL FRAMEWORK

National Security Law (2015) 国家安全法



Cybersecurity Law (2017)
网络安全法

Data SecurityLaw (2021)
数据安全法

Personal Information Law (2021)
个人信息保护法

+ Measures, Regulations, Provisions, Standards, …etc.

BACKGROUND AND LEGAL FRAMEWORK

RGPD v. PIPL

This law, which some consider to be similar, comparable or even inspired by the RGPD, has several differences.

- ✓ Although this law allows data to be processed under contractual or legal obligation, the concept of legitimate interest is absent and it will generally be necessary to obtain consumer consent.
- ✓ The PIPL focuses more on where the personal information processing activity happens.
- ✓ The PIPL excludes anonymous information from the definition of PI.
- ✓ The PIPL has a much wider scope of what is considered “sensitive” PI than GDPR’s “special category” data.
- ✓ The GDPR defines the roles of the data controller and data processor, while the PIPL defines the role of PI handler (which is the same as the data controller) but not a data processor (which is sometimes referred to as the “entrusted party”).
- ✓ The PIPL calls it a Personal Information Protection Impact Assessment (PIPIA), while the GDPR calls it Data Protection Impact Assessment (DPIA); etc.

The state is not subject to the law

The general philosophy/purpose of the legal regime is not that adopted by Europe

The economic and strategic stakes are higher than in Europe

RGPD v. PIPL : Applicable scope

Both the GDPR and the PIPL are extraterritorial in application; The GDPR focuses more on where the business is established, while The PIPL focuses more on where the personal information processing activity happens.

RGPD v. PIPL : Definition of Personal information

Both the GDPR and the PIPL have a similar definition for general PI, either direct or indirect and define similar rights for individuals; some categories of PI are subject to more stringent protection requirements – “special category” data in the GDPR and “sensitive” PI in the PIPL. The PIPL excludes anonymous information from the definition of PI. The PIPL has a much wider scope of what is considered “sensitive” PI than GDPR’s “special category” data.

RGPD v. PIPL : Supervisory authorities

Under the GDPR, there is usually a single and independent supervisory authority with a clearly defined regulatory scope and supervisory procedures while multiple supervisory authorities exist in China with interrelated responsibilities.

RGPD v. PIPL : Cross Border Data Transfer

Both the GDPR and the PIPL request the recipient party to provide adequate protection for the PI they receive and that the level of protection should be equivalent to the requirements of the GDPR or the PIPL. The GDPR defines a few channels for cross-border data transfer (CBDT), which include “adequacy decision” (for destination country), SCC, and BCR (for MNCs). And GDPR allows CBDT when obtaining explicit consent from the data subject, for public interest, or for purposes of performing a contract. The PIPL’s CBDT rules are binding with other laws, such as the CSL and the DSL and requests the CBDT on the basis of “security assessment”, “certification”, or “standard contract with the recipient”.

RGPD v. PIPL : Data protection impact assessment

The PIPL calls it a Personal Information Protection Impact Assessment (PIPIA), while the GDPR calls it Data Protection Impact Assessment (DPIA). The GDPR defines scenarios in which a DPIA must be conducted rather ambiguously, requiring it when processing PI with new technology, creating a high risk for the data subject. The PIPL defines the scenarios in which a PIPIA must be conducted more specifically.

MAIN ACTORS INVOLVED

Cyberspace Administration of China (CAC):

The most important regulator of China's internet, responsible for all work related to cyberspace, and with a central role in overseeing the CSL, DSL and PIPL.

Through its provincial-level offices, CAC is also responsible for conducting security assessments for cross-border data transfers. In addition, CAC hosts the Party's Office of the Central Cyberspace Administration Commission.

Ministry of Industry and Information Technology (MIIT): Responsible for planning, developing, and monitoring industrial policies, infrastructure and equipment in key fields. It is also responsible for assessing and granting relevant licenses to operate in China, including for foreign companies.

Ministry of Public Security (MPS) & Ministry of State Security (MSS), mainly responsible for the investigation of illegal activities and enforcement of punitive actions.

MAIN ACTORS INVOLVED

When it comes to technical standards and specifications:

Standardisation Administration of China (SAC):

Operating under the State Administration of Market Regulation (SAMR), it participates in standard formulation and implementation work.

National Information Security Standardisation Technical Committee (TC260):

Operating under SAC but under the ultimate guidance of CAC, it is the most important body in researching and writing China's national standards in the field of cybersecurity, data and personal information.

China Electronics Standardisation Institute (CESI): Influential standard developing organisation in China, focusing on various fields such as cybersecurity, big data, smart cities, artificial intelligence, internet of things, etc. It currently hosts the secretariat of TC260 – among many other national technical committees; it also participates actively in international standardisation activities.

China Academy of Information and Communications Technology (CAICT): Influential think tank under MIIT which plays a key advisory role in the development of standards

and policies in the field of information and communication technology.

APPLICABILITY AND KEY SUBJECTS

The CSL, DSL and PIPL apply to all entities operating **in**/**with** China and dealing with Chinese organisations and individuals.

The CSL applies to established entities involved in the construction, operation, maintenance and use of networks within the territory of China (CSL, Art. 2);

The DSL applies to data processing activities, as well as to supervision and regulation of such activities, within the territory of China (DSL, Art. 2);

The PIPL applies to the processing of the personal information of natural persons within the territory of China (PIPL, Art. 3).

APPLICABILITY AND KEY SUBJECTS

At the same time, these three laws have an extraterritorial reach, extending their scope to overseas entities based abroad, targeting especially:

All data processing activities outside the territory of China that might be detrimental to the country's national security, public interest or rights of its citizens and organisations (DSL, Art. 2);

All entities outside the territory of China yet processing the personal information of natural persons located within China with the aim of: providing products and services to natural persons located in China, analysing or assessing their conduct, or under any other circumstances as provided by any law regulation (PIPL, Art. 3.2).

Hence, EU SMEs falling under this scope will need to comply with Chinese laws and regulations even without a legal presence in China.

APPLICABILITY AND KEY SUBJECTS

The CSL, DSL and PIPL, also distinguish among different **subjects and roles**:

Network Operators (NOs)

网络运营者

NOs are owners and administrators of networks, and network service providers. Network

refers to systems that are used for the purpose of collecting, storing, transmitting, exchanging, and processing information (CSL, Art. 76). In practice, companies that provide services or operate through networks (e.g., websites, ERP, etc.) are also considered NOs.

Providers of network products and services

网络产品、服务的提供者

Providers, manufacturers, and integrators of network products and services that are used by NOs and CII operators.

These include: computers, communication equipment, information terminal, industrial control network equipment, system software, application software, etc. (GB/T 39276-2020).

Critical Information Infrastructure (CII) operators

关键信息基础设施的运营者

Entities operating important network facilities and information systems in key areas (e.g., public communication, energy, transport, water, finance, etc.) that may endanger national security, economy, people's livelihood and public interests in the event of destruction, loss of function or disclosure of data (CSL, Art. 31).

APPLICABILITY AND KEY SUBJECTS

Each of these subjects must comply with specific obligations and requirements.

Foreign invested companies operating in China with EU companies as shareholders may fall under all these definitions.

Furthermore, with regards to data and personal information, the following subjects and roles can also be distinguished (next slide) .

EU companies may fall under all these definitions, but they should be aware of the terminology difference with other data protection laws, especially the EU GDPR.

Data / PI processor 数据 / 个人信息处理者

Entity or individual collecting, storing, using, processing, transmitting, providing, publishing and erasing data or PI. It also refers to the party who control and determines the purpose and method of data processing – similar to 'data controller' under the GDPR

Entrusted party 受托人

Party processing data or PI on behalf of, and at the instruction of, the PI processor – similar to 'data processor' under the EU GDPR.

Offshore receiver 境外接收方

Foreign party receiving data or personal information from a China-based processor, involved in further processing activities.

DEFINITIONS AND CLASSIFICATION OF DATA & PERSONAL INFORMATION

CORE DATA

Data concerning national security, the lifeline of the national economy, important livelihood of people, or major public interest. Core data is subject to the highest degree of protection and management system

IMPORTANT DATA

Important data refers to data that, if tampered with, leaked, compromised, or illegally acquired or used, may cause harm to national security or public interest. It cannot be transferred over-seas without a government security assessment

GENERIC DATA

All other data that is neither core data nor important data

SENSITIVE PERSONAL INFORMATION

Personal information that once leaked, illegally provided or abused, could endanger personal and property safety, or easily lead to damages to personal reputation, mental and physical health, discrimina-tory treatment, etc.

It also includes personal information of minors under 14 years of age.

PERSONAL INFORMATION

Any information that is recorded, electronically or otherwise, that can be used alone or in combinaison with other information to identify a natural person or reflect the activity of a natural person. It does not include personal information after anonymisation.

PERSONAL INFORMATION PROTECTION REQUIREMENTS

The PIPL outlines (Art. 5-9) seven fundamental principles on which PI processing activities must be grounded:

(i) legality;
(ii) clarity and reasonability of the purpose;
(iii) minimum necessity of collection;
(iv) openness and transparency;
(v) accuracy and quality;
(vi) accountability;
(vii) security.

At the same time, PI processing activities are allowed only when conforming to specific circumstances. And PI processors must strictly follow several requirements and procedures both before and during their PI processing activities.

PERSONAL INFORMATION PROTECTION REQUIREMENTS

Collection, storage, use, processing, transmission, provision, publishing and erasure of PI are allowed only when conforming to one of the circumstances :

- ✓ **Voluntary consent** of the individual obtained under the precondition of full knowledge, explicit statement; consent might be rescinded by the individual;
- ✓ Necessity to fulfil a contract where the individual is a party, or for lawful **human resources management** according to laws and regulations;
- ✓ Necessity to **fulfil legal duties**, responsibilities or obligations;
- ✓ Necessity to respond to **public health** incidents or protect life and property;
- ✓ News reporting or **public interest** activities – but within a reasonable scope;
- ✓ Information disclosed by the individual or otherwise **already disclosed** in a lawful manner – but within a reasonable scope.

PERSONAL INFORMATION PROTECTION REQUIREMENTS

Before processing activity, PI Processors must inform relevant individuals of the following items – in truthful, accurate, clear, noticeable, and easy-to-understand language:

- Name and contact information of the PI processor;
- Purpose, methods of PI processing;
- Type of PI processed;
- Retention period;
- Methods and procedures for individuals to exercise their legitimate rights;
- Other matters according to laws.

If the above items are disclosed through PI processing rules, these shall be public and easily accessible.

PERSONAL INFORMATION PROTECTION REQUIREMENTS

During processing activity, PI Processors must fully respect the following legitimate rights of individuals:

- To be informed;
- To restrict or object to certain processing;
- To timely access and obtain a copy of the PI processed;
- To rectify and delete incorrect information upon request;
- To receive an explanation of data processing rules;
- To transfer the above rights to close relatives in case of death.

PI Processors must prevent unauthorised access, leaks, distortion or loss, by:

- Formulating internal management systems and SOPs;
- Implementing categorised management of PI;
- Implementing technical security measures, e.g., encryption, anonymisation, etc.;
- Determine operational limits for PI processing;
- Conduct regular training for employees on PI protection;
- Implementing emergency and incident response plans;
- Participating in regular PI compliance audits.

PERSONAL INFORMATION PROTECTION REQUIREMENTS

PI processors based outside the territory of China and subject to PIPL's extra-territorial reach (Art. 3.2) shall establish a dedicated entity or appoint a representative within the borders of China and are to report the name of the relevant entity or the personal name of the representative and contact method, etc., to the departments fulfilling personal information protection duties and responsibilities.

If the PI processed by the processor exceeds the quantitative threshold of one million individuals, the processor will be subject to stricter requirements and procedures for cross-border data transfer.

Appointment of a PI protection officer responsible for supervising all PI processing activities and localised storage within the territory of China are recommended practice by national technical standards or draft of regulations.

If the PI processed is considered sensitive personal information, additional obligations will apply to the processor (Art. 28 to 32 of PIPL). Most importantly, sensitive personal information may be processed only when there is a specific purpose and necessity, and when strict protecting measures are taken. For instance, the PI of minors under the age of 14 requires their parents' or guardians' consent; the processors must also conduct a PI protection impact assessment in advance and record the processing situation.

DATA STORAGE AND CROSS-BORDER TRANSFER REQUIREMENTS

The CSL, DSL, PIPL, and subsequent regulations and rules put forward specific requirements for localised storage and cross-border transfer of data and personal information processed in China. China is one of the countries with the most restrictive data governance regimes globally.

Data localisation is mandatory for CII operators and a recommended practice for processors of important data and for processors of personal information above the threshold of 1 million individuals.

Specifically, Art. 37 of the CSL stipulates that CII operators must store within the territory of China all important data and personal information processed therein.

Even though there is no explicit mention of non-CII operators, it can be reasonably assumed that any processors of such data are expected to store it within China. This is confirmed, for instance, by relevant regulations in specific sectors, such as automotive, which require that important data in the automotive industry is stored within China.

DATA STORAGE AND CROSS-BORDER TRANSFER REQUIREMENTS

Art. 40 of the PIPL sets the requirement of data localisation to any processors of personal information exceeding the threshold of 1 million individuals, regardless of whether the processor is a CII operator or not.

Therefore, PI processors below the threshold – to which the majority of EU SMEs belong – are not required to store personal information within the territory of China; **but they will still need to follow specific requirements and procedures when transferring overseas the PI processed in China.**

In addition to these requirements, similar data localisation requirements may be in place for data processing activities within certain industries – such as banking and finance, geology, genetics, etc.

For instance, the Administrative Measures for Population Health Information provides that medical, health and family planning service agencies may not store population health information on any server outside China and may not host or lease any server outside China. Measures for the Administration of Scientific Data and the Regulations for the Management of Human Genetic Resources, scientific data produced under any government-funded project and all genetics data must be stored within China, cannot be published in international journals without prior approval, and must be shared with Chinese collaborators.

DATA STORAGE AND CROSS-BORDER TRANSFER REQUIREMENTS

Similar to data localisation, there are specific requirements and procedures for transferring overseas data and personal information processed in China, depending on the nature of the processor and the type of data.

	CII operators	Non-CII operators (+ 1 M indiv.)	Non-CII operators (- 1 M indiv.)
DATA (Important)	Security Assessment	Security Assessment	Security Assessment
PI	Security Assessment	Security Assessment	Security Assessment Certification Scheme Standard Contract

Exceed cumulative threshold of PI transferable overseas?

100 000 personal information or 10 000 sensitive personal information since 1st January of the previous year.

Method 1: CAC security assessment

The CAC-led security assessment is the only possible cross-border transfer method for:

- *Any entity transferring important data from China to overseas – regardless of the amount of data to be transferred;*
- *CII operators, as well as non-CII operators processing personal information above the threshold (1 million individuals);*
- *Any entity, including non-CII operators below the threshold, transferring overseas a cumulative amount of personal information of more than 100,000 individuals, or sensitive personal infor-mation of more than 10,000 individuals, counted from 1st January of the previous year;*
- *Other cases deemed necessary by China's cyber-security authorities.*

It is mandatory that the security assessment is conducted **before** the cross-border data transfer activity begins. The results of each security assessment are valid for two years.

Remote access from a foreign country to important data and PI stored within the territory of China will be considered a cross-border data transfer.

Method 2: Standard Contract Provisions

If the security assessment prior to cross-border data transfer is not mandatory, personal information exporters may use the Standard Contract Provisions issued by CAC. Hence, this method can only be chosen if the PI exporter satisfies **all** the conditions below:

- *Is not a CII operator;*
- *Is an entity processing personal information below the threshold (1 million individuals);*
- *Has not transferred overseas, cumulatively since 1 January of the previous year, PI of more than 100 000 individuals, or sensitive personal infor-mation of more than 10 000 individuals.*

The specific requirements are detailed in the draft Standard Contract Provisions for the Cross-Border Transfer of Personal Information, released by CAC in June 2022.

Eligible PI processors must conduct a Personal Information Protection Impact Assessment (very similar to the Data Protection Impact Assessment under the GDPR.)

Method 3: Certification scheme

In alternative to the Standard Contract Provisions, non-CII operators processing PI below the threshold (1 million individuals) may choose to apply for a certification for the cross-border transfer of personal information – which could be comparable to the EU Binding Corporate Rules under the GDPR. The specific requirements and processes for doing so are detailed in the Certification Requirements for Cross-border Transfer of Personal Information, issued by TC260 in June 2022.

Specifically, certification can be obtained for two types of cross-border transfer of personal information:

- **Cross-border transfer of personal information between subsidiaries and affiliated companies of multinational companies or other economic organisations;**
- **Personal information processing activities that are subject to PIPL's extraterritorial reach.**

Certification scheme appears more appropriate for PI transfers between European headquarters and China-based subsidiaries using standardised procedures and clear data flows.

In practice, it remains to be seen how this will be enforced as it seems unlikely that foreign companies will apply voluntarily for certification.

PENALTIES FOR NON-COMPLIANT CASES

Violating the obligations and requirements of cyber-security, data security and personal information protection may trigger administrative, civil, or even criminal liabilities.

Under certain circumstances, not only the organisation but also responsible individuals may be punished.

- ✓ Cybersecurity violations normally range between RMB 5 000 and RMB 1 million;
- ✓ Data breaches in connection to personal information may take up to RMB 50 million or 5% of the global turnover.
- ✓ Penalties generally up to RMB 5 million are also applicable for violation of cross-border data transfer requirements.
- ✓ Penalties may be drastically higher in case of multiple violations of different laws and regulations.
- ✓ At the same time, in addition to monetary fines, other forms of punishment may also involve aspects such as the closure of online offerings, suspension or revoking of business permits and licenses, etc.

PENALTIES FOR NON-COMPLIANT CASES

It must be kept in mind that penalties will also apply to overseas entities which are subject to the extraterritorial reach of the DSL and PIPL.

Yet,if such entities do not have a legal presence in China, enforceability might be challenging – unless severe violations are concerned, which might lead to the direct involvement of the Ministry of State Security and Ministry of Public Security, or also through bilateral agreements with overseas authorities.

Other potentially feasible repercussions for the foreign company could involve blocking the accessibility of its website from within the territory of China, the impossibility for it to pass security assessment as an offshore receiver in future transactions with China-based data exporters, or even blacklisting in severe cases.

COMPLIANCE TIPS

DATA MAPING
… Amount & Extent of outbound flows?

DATA ASSESSMENT
… Data flows at risks of non compliance?

EMERGENCY PLAN
… contingency plan for network attack or breach of data security?

REVIEW CONTRACTS & POLICIES
… integrate amendment aligned as much as possible with PIPL..

TRAIN PERSONNEL
… employees exposed to data flows shall be informed and regularly trained.

If my company does business with China but it does not have a subsidiary there, do we still need to comply with China's cybersecurity, data and personal information protection regime?

Even if a company does not have a legal presence in China but nonetheless processes data or personal information of Chinese organisations/individuals, it still needs to comply with China's data and personal information protection regulations – including in regard with cross-border data transfer.

In particular, PI processors based abroad and subject to PIPL's extraterritorial reach will need to establish a dedicated entity or appoint a representative within the borders of China to be responsible for matters related to the PI they handle and are to report the name of the designated entity, or the name and contact method of the representative, to the departments fulfilling personal information protection duties and responsibilities.

We sell consumer products from Europe on Chinese e-commerce platforms (we do not have a subsidiary in China). Do we still need to follow China's data and personal information rules?

The company will still need to comply with China's data and personal information protection regulations – in line with the extraterritorial reach of the DSL and PIPL – as the European seller may have access to the PI of its Chinese purchasers.
Yet, most of the responsibility will fall on the Chinese e-commerce platform to lawfully process PI and use algorithms.

If the European seller wants to access personal information obtained by the Chinese e-commerce platform, the latter must strictly follow relevant procedures for cross-border data transfer.

Nevertheless, if a European seller targets Chinese customers and collects, stores, uses, processes, transfers personal information from individuals located within China, it should be compliant with PIPL.

Can I transfer important data to our company's HQs in Europe?

Important data collected and stored in China can be transferred abroad, provided that a prior security assessment is concluded positively by CAC.

This is a mandatory requirement for any type of entity, regardless of their nature (CII operator or not) and the amount of data to be transferred (no quantitative threshold).

Additional requirements and obligations might exist for specific industries.

Finally, further restrictions or bans exist for Chinese entities (including subsidiaries of foreign companies) that want to transfer intellectual property rights overseas. (Hundreds of fields listed as 'prohibited' or 'restricted' for exports in a MOFCOM-MOST catalogue, last revised in 2020, see: http://www. gov.cn/zhengce/zhengceku/2020-08/29/content_5538299.htm)

Can I transfer generic data to our company's HQs in Europe?

Generic data (i.e., data not considered core data or important data) is not subject to CAC security assessment – provided that it is not personal information above a certain threshold.

Even though generic data is further divided into different grades depending on its impact on the rights of citizens and organisations, there are no major restrictions for its transfer abroad.

Still, Standard Contract Provisions must be followed, or a certification obtained – the latter appears explicitly directed to cross-border transfers of generic data among entities belonging to the same business group.

How should we interpret the 1 000 000 / 100 000 / 10 000 quantitative thresholds for personal information processing and cross-border transfer? Do these refer to single data entries or subjects?

Relevant regulations and standards do not provide a clear indication of whether personal information (e.g. the name, surname, age and bank details of an individual) are counted as single entries (4 items of personal information) or based on individual data subjects (1 item of personal information).

As a definite answer is not available at this stage, EU companies are advised to make a comprehensive mapping and quantification of the information collected and plan actions in line with relevant obligations, requirements and risks.

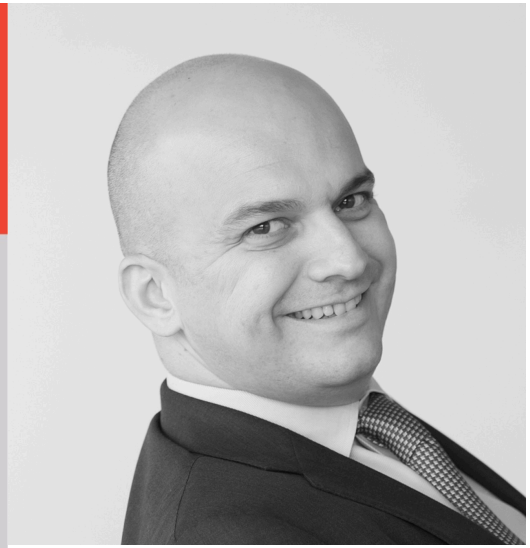
Are website cookies considered personal infor-mation? Can I transfer such information to our HQs in Europe for analytics and planning purposes?

It depends on what kind of information the cookies collect.

If they collect personal identified and/or identifiable information, then website cookies are considered personal information.

Hence, in order to continue using them, website managers must follow the obligations and requirements, specifically informing the visitors of the website (in a clear and accurate manner) and asking them to give or refuse consent before any PI processing activities begins.

This applies to cookies used for any purpose, including advertisements, e-commerce, or analytics and also covers the personal information of website visitors such as account names, logos, avatars, etc.



Franck DESEVEDAVY

Franck Desevedavy exerce à titre principal en Chine, à Hong Kong et à Taiwan depuis 1996.

Il est un spécialiste du droit des investissements étrangers dans ces territoires,
outre un praticien reconnu du droit de la propriété intellectuelle,
et du contentieux arbitral et judiciaire - civil, commercial et pénal.

Après une première expérience d'interprète français-chinois pour la 12ème section des Rens. Gén. Paris,
suivie de deux années à Paris dans un cabinet d'avocats généralistes,
Franck Desevedavy a été associé de cabinets taïwanais puis français en Asie,
avant d'être l'un des cofondateurs du cabinet ASIALLIANS.

Au-delà de ses activités professionnelles, Franck enseigne régulièrement le droit chinois
devant des étudiants français et le droit français devant leurs homologues asiatiques.

Avocat à la Cour de Paris
Avocat au Barreau de Taipei
Foreign Lawyer, The Law Society of Hong Kong
Autorisé à pratiquer en République Populaire de Chine

Arbitre — *CCI Paris*, *CAA Taiwan*, *CIETAC Beijing*, *SHIAC Shanghai*

Conseiller du Commerce Extérieur de la France (Taiwan)
Ancien Président du Comité Taiwan des CCEF

Premier Vice-Président de l'Association Franco-Chinoise de Droit Économique – AFCDE Paris

Vice-Président de l'Association Pour la Promotion de l'Exercice des Avocats à l'Etranger (APPEAL-E)

Membre Fondateur du Cercle K2
Représentant pour la Chine, Hong Kong et Taiwan du Cercle K2

Représentant pour la Chine, Hong Kong et Taiwan du réseau d'avocats africains ABLE

Franck DESEVEDAVY

Beijing Office: Franck.Desevedavy@asiallians.com

Tel : +86 10 8523 6016

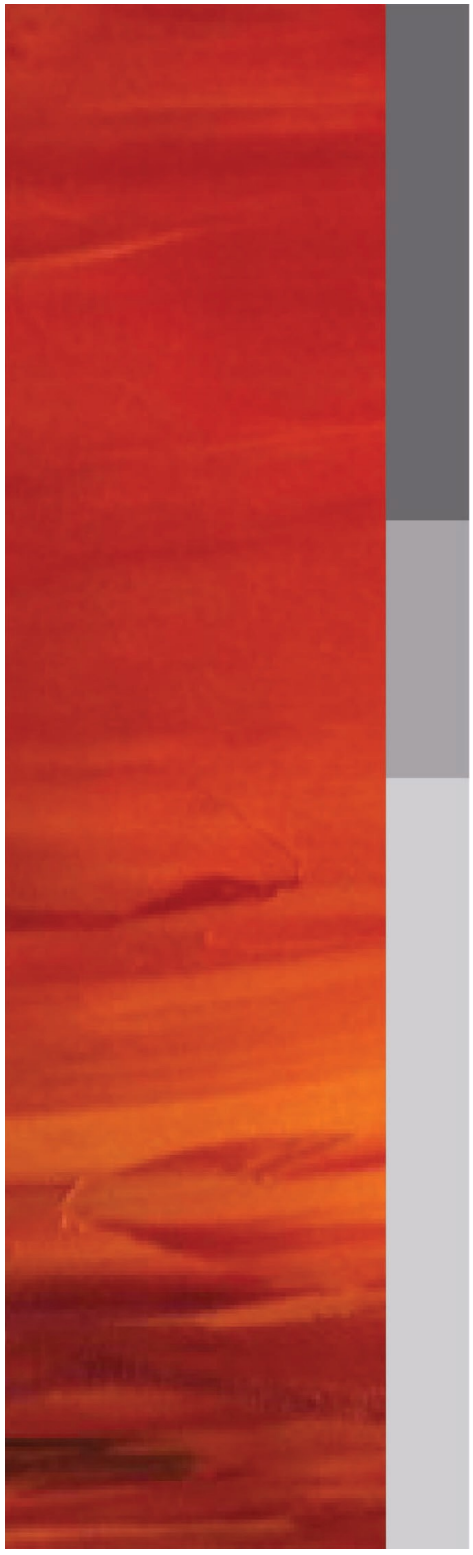
Suite 304, 3F, Building 81,
No.4 Gongti North Road,
Chaoyang District,
Beijing 100027, PRC

Paris Office: paris@asiallians.com

Tel : +33 1 73 54 95 95

189 boulevard Saint-Germain
75007 PARIS

www.asiallians.com



ASIALLIANS