EUSME Centre

Compiled in partnership with

Camera di Commercio Italiana in Cina
中国意大利商会
China-Italy Chamber of Commerce

Cybersecurity, Data & Personal Information Compliance

for EU SMEs in China

SEPTEMBER 2022

Funded by the European Union

This EU SME Centre report was written by:

Alessio Petino: Business Advisor, EU SME Centre

Arvid Tilner: Project Assistant, EU SME Centre

Reviewed by:

Valentino Lucini: Of Counsel, Wang Jing & GH Law Firm

This EU SME Centre report is an update of a previous report produced in 2020, "Personal Information and Cybersecurity Protection in China"*: https://www.eusmecentre.org.cn/guideline/personal-information-and-cybersecurity-protection-china.*

This publication was produced with the financial support of the European Union and its contents are the sole responsibility of the EU SME Centre. The views expressed in this publication do not necessarily reflect the views of the European Union.

Contents

Cybersecurity, Data and Personal Information Compliance for EU SMEs in China

EXECUTIVE SUMMARY

The security of data, together with its flow and accessibility across borders, is a fundamental element of business and innovation activities. Companies constantly use data generated from R&D or collected from customers in different locations to improve their products or develop new ones, often relying on teams based in other countries.

Over the past years, China has made significant efforts to strengthen its governance system for cybersecurity, data, and personal information protection. Complementing the *Cybersecurity Law* (CSL), the *Data Security Law* (DSL) and the *Personal Information Protection Law* (PIPL) came into effect at the end of 2021, stipulating a series of obligations not only for actors based in China but also for those based elsewhere yet processing data generated in China or personal information of Chinese citizens. These obligations also cover basic practices such as uploading Chinese data into clouds hosted abroad, managing Chinese human resources, or selling products through Chinese e-commerce platforms. As a result, many EU SMEs operating in/with China reached out to the EU SME Centre with questions about whether they would be able to continue their businesses as usual. In practice, **though facing higher compliance requirements and costs, and except for certain data-intensive sectors** (such as ICT, automotive and life sciences), **EU SMEs are less affected than Chinese domestic companies and large MNCs** – especially if they already comwply with the GDPR. This report illustrates why.

After introducing the legal framework, its applicability as well as terminology, this report digs into the specific provisions of China's CSL, DSL, and PIPL, as well as other key regulations, departmental rules and technical standards which are gradually shaping China's governance system. The aim is to provide a **practical and easy-to-navigate overview of the compliance requirements that EU SMEs need to follow**, from the perspective of cybersecurity, data security and personal information protection. Special focus is dedicated to:

- **Localised data storage requirements** – usually not applicable to EU SMEs as they are not Critical Information Infrastructure operators nor process generic data nor personal informationbelow a certain threshold;
- **Cross-border data transfer procedures** – with most SMEs being in the position to use the least strict methods, i.e., Standard Contract Provisions or certification, instead of security assessment;
- **Compliance tips and actions** that EU SMEs should take to prevent disruptions to their businesses in China.

The third section of this report also includes a list of 15 **Frequently Asked Questions**, focusing on practical issues and scenarios commonly encountered by EU SMEs. These include, for instance, how to upload on servers hosted abroad information from Chinese business activities or staff, how to deal with website cookies, how to limit impact through anonymisation of personal information, whose responsibility is engaged when working with third-party vendors, what requirements SMEs must follow when selling via Chinese e-commerce platforms, etc.

Finally, two annexes complement this report. The first is a detailed list of the factors that **guide the identification of important data** – indeed one of the key issues that have received the highest degree of attention by European companies in China; the second annex provides a detailed overview of how networks, data and personal information are further categorised into different classes and grades based on their risk and impact – e.g., the cybersecurity Multi-Level Protection Scheme 2.0.

I. BACKGROUND AND LEGAL FRAMEWORK

The digital economy has become one of China's key drivers of development and growth. Digital technologies now represent essential parts of the daily lives of Chinese citizens and companies. Chinese tech giants have gradually become global champions, launching products on overseas markets or listing on foreign stock exchanges – processes which have occasionally involved data misuse and privacy violation.

In line with these developments, 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*,[1] it represents a model of governance where the Chinese state has the ultimate authority in the cyberspace, not only within its boundaries but also on international activities affecting its national security, public interests and rights of its citizens and organisations. At the highest juridical level, China's legal framework is composed of three pillars, mostly addressing issues from the broader perspective:

- ***Cybersecurity Law*** **(CSL)**, which came into effect in June 2017, is the first omnibus law governing cybersecurity and information protection, enshrining the concept of cyber sovereignty in its first article, and outlining various obligations for network operators, internet service providers, platform operators, digital products and services, and critical information infrastructure operators.[2]

- ***Data Security Law*** **(DSL)**, which came into effect in 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.[3]

- ***Personal Information Protection Law*** **(PIPL)**, which came into effect in 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.[4]

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

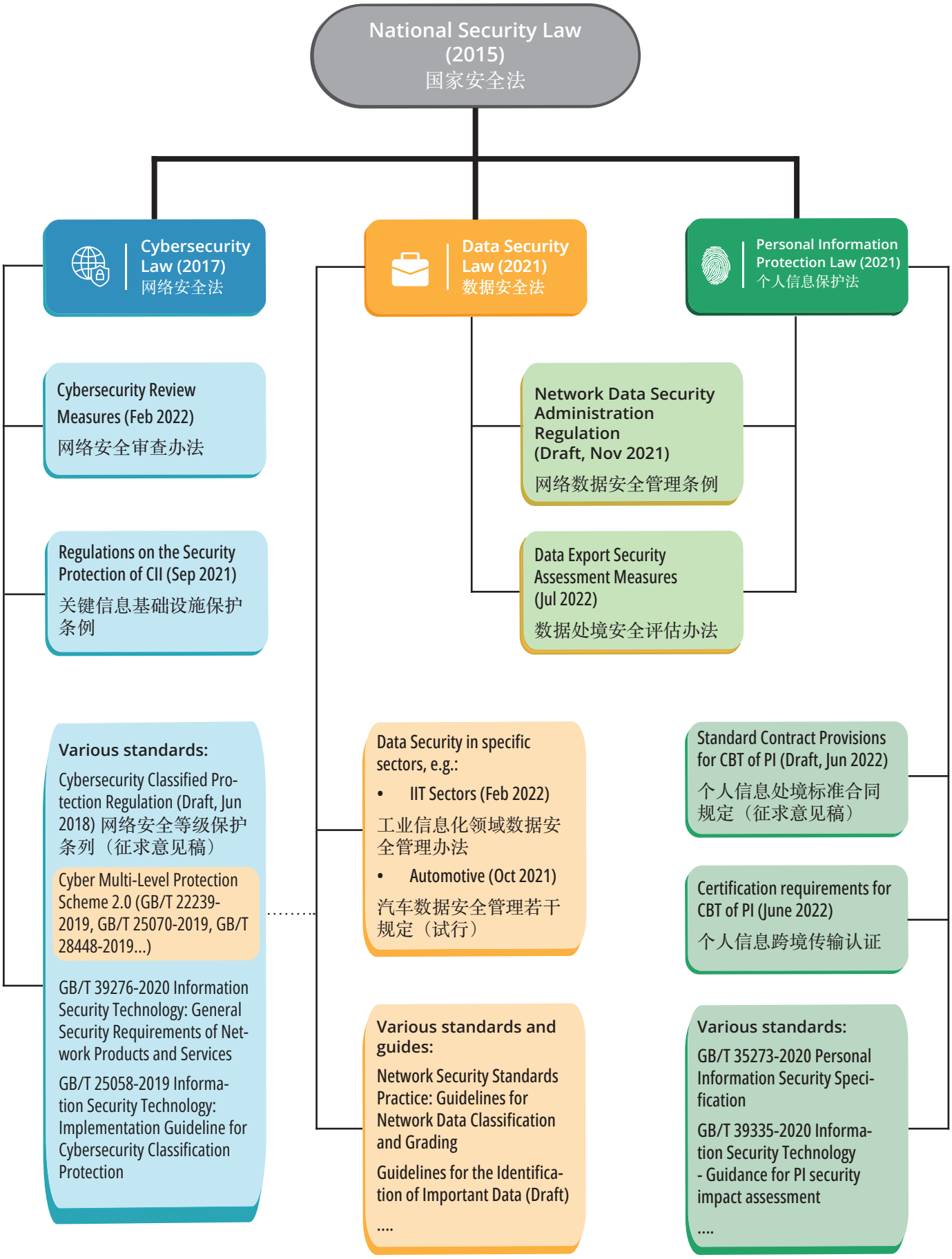
The following diagram provides a **visual mapping** of China's legal framework in the field of cybersecurity, data, and personal information protection. It only includes regulations with the highest implications for EU companies, which are mostly covered in this report. Several others exist, addressing other aspects (e.g., encryption) or specific sectors (e.g., ICT, automotive, cloud computing, etc.): those will not be covered in this report, though comprising even have much stricter requirements.

1 Specifically, Art. 25 of the *National Security Law* stipulates that China "will strengthen network management, will prevent, stop and punish network crimes such as network attacks, network intrusions, network theft, and dissemination of illegal and harmful information in accordance with the law, so as to safeguard the sovereignty, security and development interests of the country's cyberspace". See: http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm (accessed: 25 August 2022).

2 http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm (accessed: 25 August 2022).

3 http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml and its official translation in English: http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml (accessed: 25 August 2022).

4 http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (accessed: 25 August 2022).



Source: EU SME Centre

1.1 MAIN ACTORS INVOLVED

Different government bodies are involved in China's cybersecurity, data, and personal information protection legal framework:

- **Cyberspace Administration of China (CAC)**: The most important regulator of China's internet, responsible for all work related to cyberspace, and thus 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, including telecoms, internet, automotive, etc. It is also responsible for assessing and granting relevant licenses to operate in China, including for foreign companies. Its provincial-level offices are responsible for supervising the daily operations of critical information infrastructure in their areas of competence.

- Other key central-level bodies are the **Ministry of Public Security (MPS)** and the **Ministry of State Security (MSS)**, mainly responsible for the investigation of illegal activities and enforcement of punitive actions.

- Other bodies are involved in digital-related issues in their specific sectors, such as the Ministry of Transport, the Ministry of Science and Technology, etc.

When it comes to technical standards and specifications, the most important actors are:

- **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.[5]

- **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.

Information on new standards issued or open for comments are regularly published on the websites of these organisations, usually in the 'Notices and Announcements' sections or 'Calls for Comments on Standards'.

5 For an overview of TC260's cybersecurity standards currently under development and implementation, see (in Chinese): https://std.samr.gov.cn/search/orgDetailView?tcCode=TC260 (accessed: 25 August 2022). TC260 also has an official website: https://www.tc260.org.cn/ (accessed: 25 August 2022).

II. KEY REGULATORY CONTENT AND REQUIREMENTS

This section provides a summary of China's existing framework of cybersecurity, data and personal information protection laws, regulations, rules and technical standards. The content is specifically tailored to the needs and requirements of EU SMEs, in order to guide them through the dense legal framework and help them to be fully compliant when doing business in China or with Chinese companies or individuals.

2.1 APPLICABILITY AND KEY SUBJECTS

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

- 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).

At the same time, these three laws have an **extra-territorial 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**. A dedicated entity or representative must be appointed in China by overseas PI processors. Despite this, in such cases, monitoring non-compliant cases and enforceability will be challenging, and detailed measures will remain to be seen in actual practice (more details are provided in section 2.5 and the FAQs).

The CSL, DSL and PIPL, as well as their implementing rules and standards, also distinguish among different **subjects and roles**. Specifically:

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.

Can foreign-invested companies be Network Operators? Yes!

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 seriously 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).

Can foreign-invested companies be CII operators? In principle yes, but not likely (see FAQs)

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).

Can foreign-invested companies be providers of network products and services? Yes!

Each of these subjects must comply with **specific obligations and requirements** (to be detailed in section 2.3). Foreign invested companies operating in China with EU companies as shareholders may fall under all these definitions – though in the case of CII operators it is not particularly likely, especially for SMEs.

Furthermore, with regards to data and personal information, the following subjects and roles can also be distinguished. 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**

Can foreign-invested companies be PI Processors? Yes!

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**

Can foreign-invested companies be entrusted parties? Yes!

Offshore receiver
境外接收方

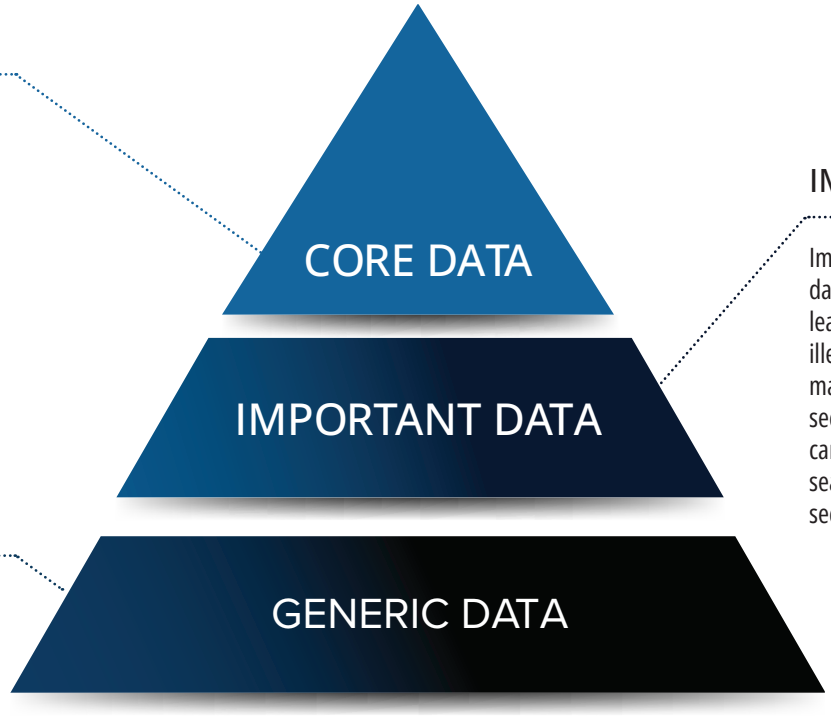
Foreign party receiving data or personal information from a China-based processor, involved in further processing activities

Can foreign-invested companies be offshore receivers? Yes!

2.2 DEFINITIONS AND CLASSIFICATION OF DATA AND PERSONAL INFORMATION

The Chinese legal framework provides different definitions, classifications and grades of data and personal information – each requiring different levels of security and protection by the relevant processors. For instance, for data, the **following types of data** are distinguished:

Types of data



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 overseas without a government security assessment

GENERIC DATA

All other data that is neither core data nor important data

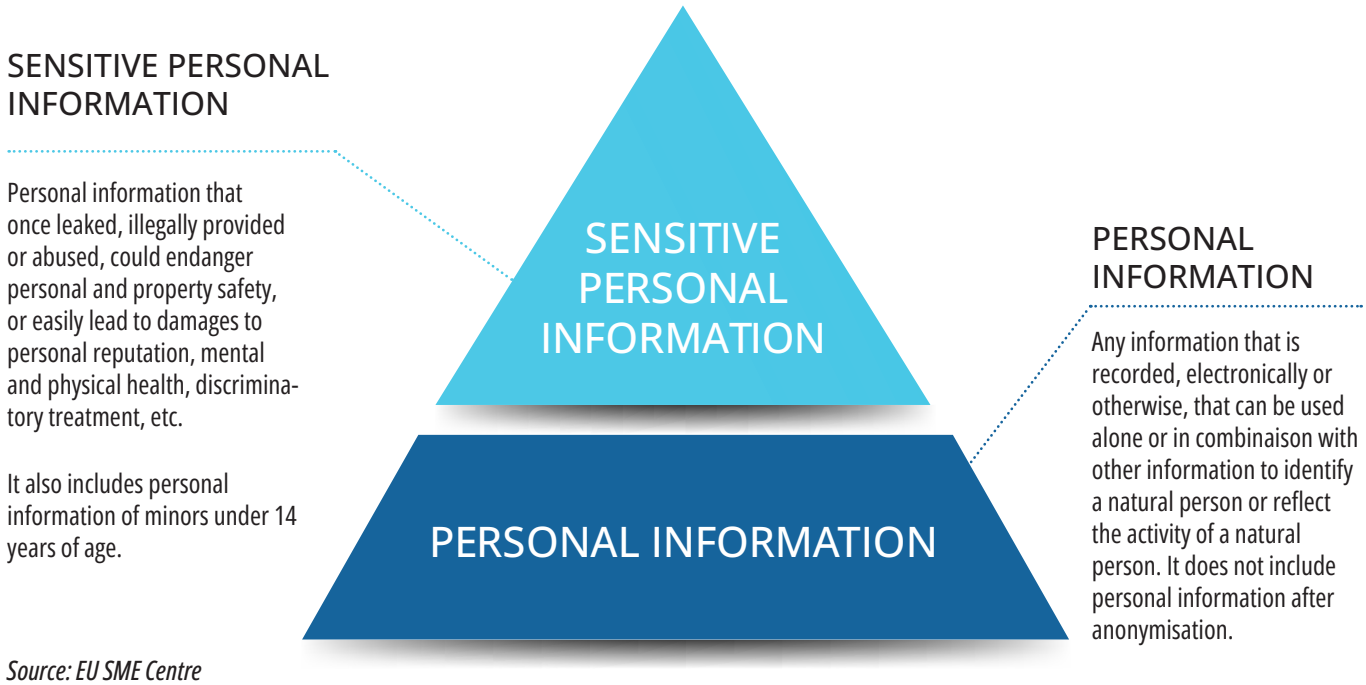
Source: EU SME Centre

In January 2022, TC260 issued **draft guidelines for the identification of important data**, specifically outlining a set of principles and key factors to guide relevant actors to assess the importance of the data processed.[6] In general, the following types of data are considered important data:

- Business information related to Chinese clients who are CII operators;
- Data and technical information involving items under export control, such as dual-use items, nuclear-related, etc;
- Data involving undisclosed information obtained from/on government agencies, military organisations or targets;
- Data involving China's national resources, environment, and population;
- Data involving critical strategic materials, components and relevant supply chains.

Hence, in general, **data that are only important or sensitive to the organisation itself, without implications on national, public and social interests, are not considered important data; the same applies to trade secrets protected as such by companies**. A detailed list of the principles and factors for identifying important data is provided in Annex 1 of this report; **practical examples** are also included in the FAQs section. It is noteworthy that detailed guidelines for the identification of important data are being formulated by competent authorities for specific industries (e.g., automotive and ICT sectors) and regions.

With regards to personal information (PI), the PIPL provides the following definitions and classification:



Source: EU SME Centre

Examples of PI include (but are not limited to): an individual's name, date of birth, ID number, biometric information, residential address, contact information, communication records and content, residence and property information, credit information, health and physiological information. Furthermore, information such as user profiling, features, or labels, are also considered PI if, after processing, it might still identify a particular natural person or reflect the activity of a particular natural person. The standard GB/T 35273-2020 Personal Information Security Specification, issued in 2020 by TC260, offers in its annexes detailed examples of PI, as well as identification and safeguard methods.[7]

6 https://www.tc260.org.cn/file/2022-01-13/bce09e6b-1216-4248-859b-ec3915010f5a.pdf (accessed: 25 August 2022)

7 https://www.tc260.org.cn/piss/files/zwb.pdf (accessed: 25 August 2022). An English translation was also produced by TC260: https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf (accessed: 25 August 2022).

Depending on the amount of PI processed, processors will have different obligations in terms of data storage and cross-border data transfer (more details in section 2.4).

Finally, China has issued a series of standards further dividing network systems and data into different security levels, based on their importance and the impact that their infringement would have on citizens, organisations, public interest or national security. Different security levels correspond to different requirements and obligations for their operators – domestic and foreign companies alike. These standards are the **Multi-Level Protection Scheme 2.0 for networks**, and the **Classification and Grading for Data**. More details are provided in Annex 2.

2.3 OBLIGATIONS AND REQUIREMENTS

This section examines in detail the specific obligations and requirements that China's legal framework puts on relevant actors – particularly EU SMEs. It does so from the perspective of cybersecurity, data security, and personal information protection.

CYBERSECURITY REQUIREMENTS

The CSL stipulates obligations for its three specific key subjects, namely Network Operators (NOs), Critical Information Infrastructure (CII) operators, and providers of network products and services. Only the obligations for **NOs and providers of network products and services** will be detailed here – as these are the two categories where EU companies mostly fall in. It is highly unlikely that EU companies, and in particular SMEs, will be considered as CII operators (for more details on the specific obligations for CII operators, please reach out to the EU SME Centre).

Network Operators (NOs)	Obligations
Enterprises operating intranet, industrial control systems, ERPs, or simply having their own website, are considered NOs and must adopt measures to protect networks from disruption, damage, unauthorised access, data leakage, stealing or falsification. The CSL stipulates the following obligations for NOs in accordance with the security requirements of the **Multi-Level Protection Scheme** (see Annex 2).	Develop internal security management rules, systems and operating procedures to prevent bigger damages in case of a cybersecurity incident; Appoint a cybersecurity responsible person; Adopt technical measures to: • Prevent, combat and investigate cybersecurity incidents (e.g. computer viruses, cyber-attacks and invasions, etc.); • Monitor and record the status of network operations and cybersecurity incidents, pre-service relevant weblogs for at least six months; • Ensure classification, mapping, backup, encryption of important data; • Support public security organs in investigating cybersecurity crimes. Formulate emergency response plans for cybersecurity incidents; Oversee users' dissemination of information, stop services, respond and report transmission of illegal information or malware; Immediately take remedial measures when network products or services face risks, at the same time informing users and reporting in a timely manner.

Providers of network product and services	Obligations
Providers, manufacturers, and integrators of network products and services that are used by NOs and CII operators, including: computer,	Inform users, report to the authorities and take remedial measures on any **known security defects, bugs, vulnerabilities** or other product risks; Provide continuous **security maintenance** for products and services until the official termination of the agreement;

Providers of network product and services	Obligations
communication equipment, information terminal, industrial control network equipment, system software, application software, etc.	Refrain from **installing malware** or other malicious programmes; Express and obtain **user's consent** if and when collecting user information (more details on personal information later in this chapter); Additional obligations, such as confidentiality, if the network product of service is to be **procured or used by CII operators**.[8] If the user is a **network platform operator** with 1+ million users and has plans to list on foreign market, it should apply for a network security review.

DATA SECURITY REQUIREMENTS

Various obligations and requirements must be followed by all entities carrying out data processing activities within China, or data processing activities outside China which might be detrimental to the country's national security, public interest or rights of its citizens and organisations. The following is a summary of the obligations stipulated by the DSL and the draft *Network Data Security Regulations*[9] – relevant for EU SMEs which are generally involved in processing activities of generic data on basic networks, with no impact on national security or public interest (see Annex 2).

In the eventuality that the data processed by a company is identified as important data, the processor must comply with a series of additional heightened requirements, especially in terms of localised data storage, cross-border data transfer, the appointment of a data protection officer and a management body in charge of data security, and the establishment of a network system meeting at least the MLPS Security Level 3.

Data processors	Obligations
Entity or individual collecting, storing, using, processing, transmitting, providing, and disclosing data – among others. The following obligations must be followed by data processors based on the **classification and grading system for data** (see Annex 2 of this report).	Establish and maintain a data protection and security **management system**; Organise internal data security **training and emergency drills**; Adopt technical and other relevant measures to ensure data security in line with the classification and grading system for data, e.g.: • Backup, encryption and access control measures; • Risk monitoring, notification to users, reporting to authorities and remedial measures immediately after detecting data security issues. **Data transaction intermediaries** must identify the sources of the data, verify the identity of the transaction parties, and retain relevant records; Do not share locally stored data to **foreign judicial organs** without prior approval of the PRC.

8 These include, e.g., passing a cybersecurity review in line with the *Cybersecurity Review Measures*, see: http://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666430.htm (accessed: 25 August 2022); obtaining a certification if the product is included in the *Catalogue of Critical Network Equipment and Network Security Products* (currently 4 critical network equipment and 11 network security products are included, see: http://www.gov.cn/xinwen/2017-06/09/content_5201276.htm, accessed: 25 August 2022)

9 The draft *Network Data Security Regulations* were released by CAC in November 2021 (http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm, accessed: 25 August 2022). The final version is expected by the end of 2022, as indicated by the Legislative Work Plan of China's State Council.

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; and (vii) security. At the same time, PI processing activities are allowed only when conforming to one of the following circumstances. At the same time, PI processors must strictly follow several requirements and procedures both before and during their PI processing activities – always ensuring that conformity and adherence to the above principles and circumstances are maintained.

PI processing activities

PI processing activities (i.e. collection, storage, use, processing, transmission, provision, publishing and erasure of PI of natural persons within China) are allowed *only when conforming* to one of the circumstances listed to the right.

Circumstances allowing PI processing activities

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.

PI processor – *Before* processing activity

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.

PI processor – *During* processing activity

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.

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.

It is noteworthy that **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** to be responsible for matters related to the personal information they handle, 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 **exceeds the quantitative threshold of one million individuals**, under currently effective laws and regulations, the processor will be subject to stricter requirements and procedures, such as appointing a PI protection officer, localised storage in China, and security review for cross-border transfers. **For some special sectors where PI is in high amount and mostly sensitive**, such as health, finance, and vehicle, compliance requirements are even higher and worthy of sectorial studies.

Finally, if the PI processed is considered **sensitive personal information** (see section 2.2 for the definition), 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.

2.4 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. These **make China one of the countries with the most restrictive data governance regimes** globally.

LOCALISED STORAGE OF DATA AND PERSONAL INFORMATION

Data localisation is mandatory for CII operators processing both important data and PI. For non-CII operators, localised storage is mandatory only for those processing PI above the quantitative threshold; in all the other cases, it is not mandatory — albeit encouraged by Chinese technical standards.[10] **EU SMEs are less affected by such requirements** as, in the majority of cases, they are involved in the processing of generic data only, or of personal information below the threshold, through basic networks.

Specifically, Art. 37 of the CSL stipulates that **CII operators should store within the territory of China** all important data and personal information collected and generated within the territory of China. Even though there is no explicit mention of non-CII operators, it can be reasonably assumed that *any* processors of important data are expected to store it within China.

	CII operators	**Non-CII operators** *(processing PI ABOVE the threshold of 1 million individuals)*	**Non-CII operators** *(processing PI BELOW the threshold of 1 million individuals)*
Important data	Localised storage	Recommended localised storage	Recommended localised storage
Personal information	Localised storage	Localised storage	No requirements

10 See, for instance, the PI protection policy template (annex D) of GB/T 35273-2020 Personal Information Security Specification (footnote no. 7)

In the case of personal information, Art. 40 of the PIPL sets the requirement of data localisation to 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.

It must be noted that, even if localised storage of data and PI is mandatory, **cross-border transfers may still be allowed** provided that prior security assessment is conducted (see next section). If localised storage is not required, **cross-border transfers still need to abide by specific requirements**, such as the use of Standard Contract Provisions or certification.

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 *Provisions for the Administration of Automotive Data Security (Trial)* stipulate that important data in the automotive industry must be stored within China.[11] The *Administrative Measures for Population Health Information (Trial)* provide 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. According to the *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. Indeed, such type of data is among the key factors outlined by TC260 for the identification of important data (see Annex 1).

CROSS-BORDER TRANSFER OF DATA AND PERSONAL INFORMATION

Similar to data localisation, there are specific requirements and procedures for **transferring overseas data and personal information** processed in China,

<table>
<tr><th></th><th>CII operators</th><th>Non-CII operators
(processing PI ABOVE the threshold of 1 million individuals)</th><th colspan="2">Non-CII operators
(processing PI BELOW the threshold of 1 million individuals)</th></tr>
<tr><td>Important data</td><td>Security assessment</td><td>Security assessment</td><td colspan="2">Security assessment</td></tr>
<tr><td rowspan="2">Personal information</td><td rowspan="2">Security assessment</td><td rowspan="2">Security assessment</td><td rowspan="2">Exceed cumulative threshold of PI transferable overseas? **

** 100 000 personal information or 10 000 sensitive personal information since 1st January of the previous year</td><td>Yes:

Security assessment</td></tr>
<tr><td>No:

Standard Contract Provisions

or

Certification scheme</td></tr>
</table>

11 http://www.gov.cn/zhengce/zhengceku/2021-09/12/content_5640023.htm (Art. 11, accessed: 25 August 2022).

depending on the nature of the processor and the type of data.

An overview of the three different methods for cross-border data transfer – i.e., security assessment, Standard Contract Provisions, and certification – is provided below.

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 information of more than 10,000 individuals, counted from 1st January of the previous year;
- Other cases deemed necessary by China's cybersecurity authorities.

In the above cases, **it is mandatory that the security assessment is conducted before the cross-border data transfer activity begins**. The specific requirements and processes for the security assessment are detailed in the *Measures for the Security Assessment of Cross-border Data Transfer*, which came into force in September 2022.[12] In all the other cases, alternative cross-border transfer methods might be chosen, such as the use of Standard Contract Provisions or certification.

The security assessment for relevant processors starts with a **self-assessment of the risks** of the cross-border data transfer, focusing on six main elements.[13] Once completed, the applicant submits the self-assessment report together with a **draft version of the contract** expected to be signed between the two parties, to provincial-level CACs.[14] If the application materials are complete, they are forwarded to the national-level CAC: if accepted, the **security assessment begins, focusing on seven key aspects** (summarised in the table to the right), and taking up to 45 workdays – or even more in complex cases. It is noteworthy that the second key aspect assessed relates to the laws, regulations and policies of the government of the country / region where the receiver is based, therefore this might leave room for politics-driven biases in the assessment results.

Seven key targets of security assessment

1. **Purpose, scope and method** of data transfer, including its legality, legitimacy and necessity
2. **Impact of legal environment** of the receiver's country on the security of the data, and alignment of the receiver's protection level with Chinese laws and regulations
3. **Scale, scope, type and sensitivity** of the data to be transferred, as well as risks of data tampering, destruction, leakage, loss, or illegal use
4. **Effective protection** of data security and personal information owners' rights
5. **Clear and full responsibilities** of data security protection stipulated in the two parties' contract
6. **Compliance** with Chinese laws, regulations and rules
7. **Other items** deemed necessary by Chinese national cybersecurity authorities

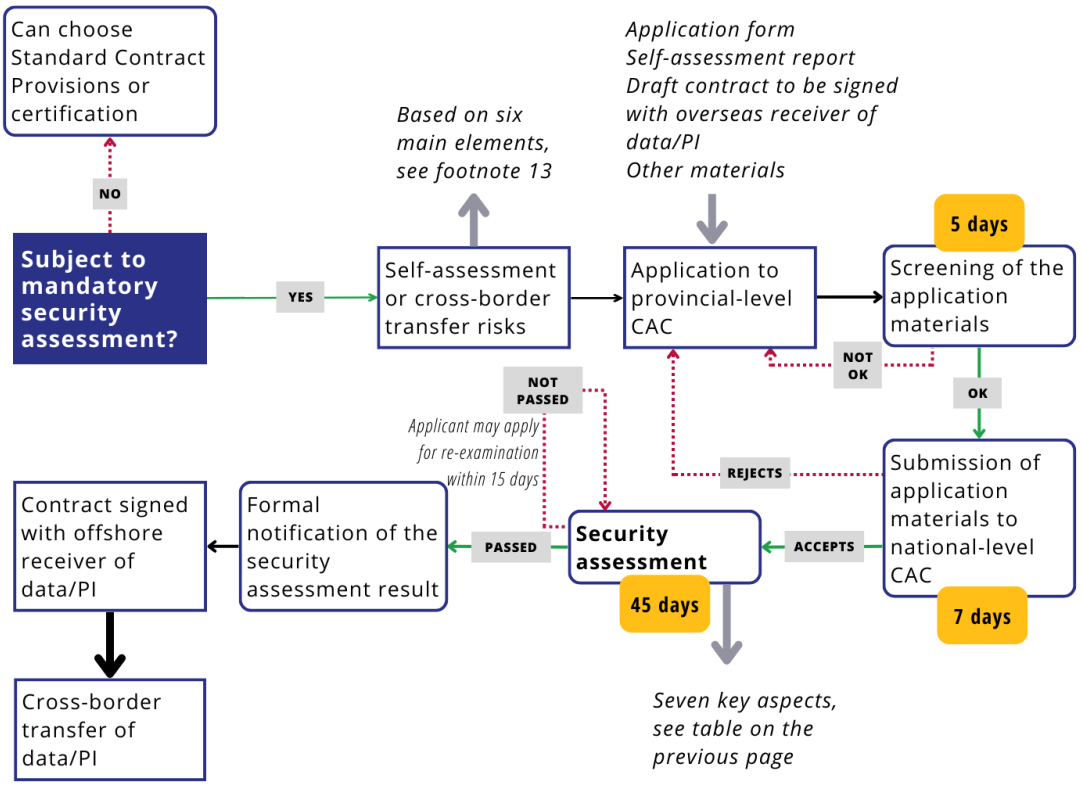
Once the assessment is complete, CAC formally notifies the applicant of the assessment result: if negative, the applicant may apply for re-examination within 15 workdays; if positive, the applicant may proceed in signing the contract with its offshore receiver, and finally, begin the cross-border transfer process. The entire process, which may take up to 3 months, is summarised in the chart on the next page.

12 http://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm (accessed: 25 August 2022).

13 Namely: (i) purpose, scope and method of the cross-border data transfer, as well as their legality, legitimacy and necessity; (ii) scale, scope, type and sensitivity of the data to be transferred, and the relevant impact on national security, public interests and rights of individuals and organisations; (iii) the capacities of the overseas receiver to ensure the security of the data once transferred; (iv) risks of data tampering, sabotage, disclosure, loss, transfer, illegal acquisition or use of the data once transferred; (v) compliance of the contract between the data processor and offshore receiver with relevant data security obligations; (vi) any other relevant aspects.

14 It is recommended to redact the contract in accordance with the Standard Contract Provisions even though the cross-border transfer is done through other methods such as CAC security assessment, certification etc. – which will be introduced in the next section.

Cross-border data transfer through CAC security assessment



Source: EU SME Centre

The results of each security assessment are **valid for two years**. An application for renewal should be submitted within 60 days before the expiration day, otherwise a new security assessment must be done again from scratch. If, in the meantime, a change in the circumstances that allowed the cross-border transfer (e.g. the purpose, the contract between the parties, etc.) occurs, the applicant will need to submit a new application.

It is noteworthy that **remote access from a foreign country** to important data and personal information stored within the territory of China will also be considered a cross-border data transfer, and thus will be subject to the above requirements. The China-based entity granting such access will be responsible for ensuring compliance.

Standard Contract Provisions (draft)

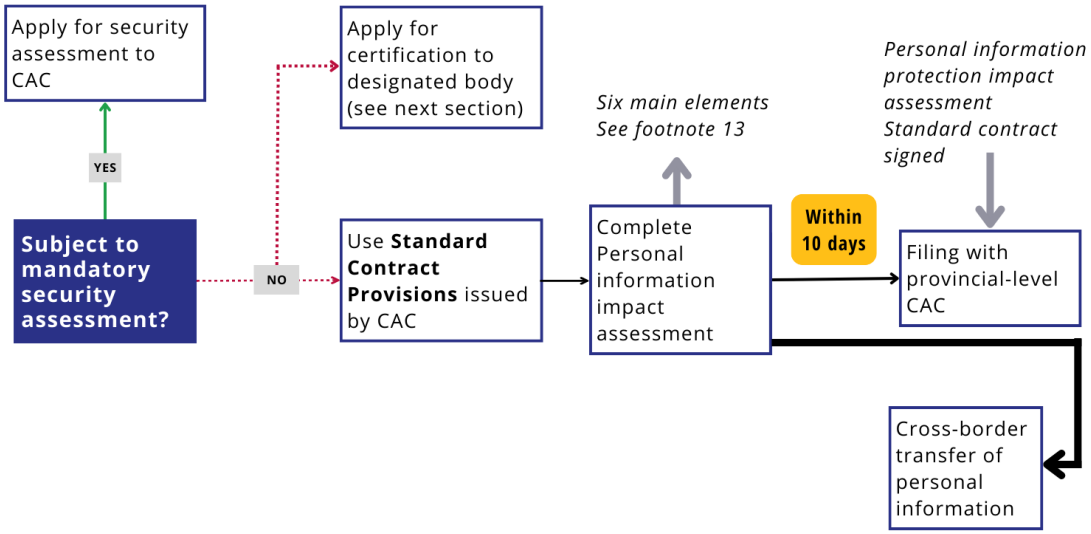
1	**Basic information** of the PI exporter and overseas receiver, e.g. name, address contacts
2	**Purpose, scope, type, sensitivity, amount, method, storage period and location** of the personal information to be exported
3	**Responsibilities and obligations** of the two contract parties, including technical and management measures adopted to prevent potential PI security risks
4	**Impact** of the policies and network of the receiver on the security of the PI
5	**Rights of PI owners** as well as ways and methods through which these are protected
6	**Relief, termination, breach, dispute settlement** of the contract between the PI exporter and overseas receiver

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 information of more than 10 000 individuals.

Cross-border data transfer through Standard Contract Provisions – based on draft regulation (June 2022)



Source: EU SME Centre

The draft specific requirements are detailed in the draft *Standard Contract Provisions for the Cross-Border Transfer of Personal Information*, released by CAC in June 2022.[15] According to the draft, eligible PI processors must first conduct a **Personal Information Protection Impact Assessment**, focused on the same six elements of the risk self-assessment that are required for the security assessment (see footnote 13); the assessment largely resembles the Data Protection Impact Assessment under the GDPR. They must also ensure that the contract signed with the overseas receiver follows the **standard provisions** (summarised in the table on the previous page) **and ideally the draft standard template provided by CAC** as annex to the document issued in June 2022. According to the current draft regulations, within 10 days after the enforcement of the contract, the PI exporter must file with provincial-level CAC the results of the impact assessment and a copy of the contract signed with its overseas receiver.

The Standard Contract Provisions issued by CAC have **significant similarities with the Standard Contract Clauses under the EU GDPR**. At the same time, however, there are certain differences: the most important relates to the fact that the applicability of China's Standard Contract Provisions is more limited, as they are applicable only if the PI exporter meets certain conditions (i.e. non-CII operator; small-scale processor of personal information) and if the exporter has not exceeded a cumulative annual threshold of PI transferred overseas (100 000 individuals, lowered to 10 000 if sensitive personal information is involved). Another significant difference relates to the fact that China's Standard Contract Provisions are limited to a China-based PI exporter and an overseas receiver, without distinguishing the different roles of processors and controllers, thus creating potential ambiguity in such scenarios. There are also divergences in terms of separate consent each time personal information is used for different purposes.

15 http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm (accessed: 25 August 2022). It is not clear when the final version will be released, and if changes will be introduced.

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, although differences exist. 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.[16]

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

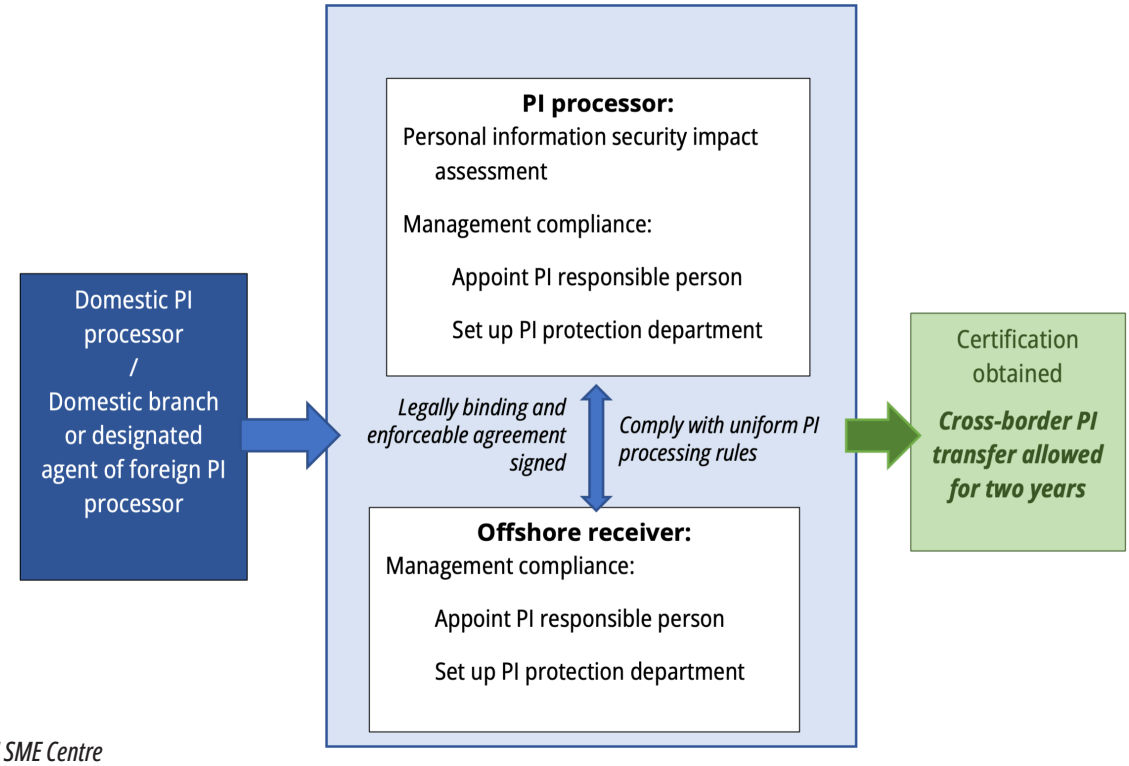
- Cross-border transfer of personal information between subsidiaries and affiliated companies of multinational companies or other economic organisations;
- Personal information processing activities that are subject to PIPL's extraterritorial reach (see section 2.1).

Therefore, the certification scheme appears **more appropriate for PI transfers between European headquarters and China-based subsidiaries using standardised procedures and clear data flows**. In such cases, the application for certification is submitted by the China-based subsidiary which acts as the PI exporter. It is noteworthy that transfers between unrelated entities will not be susceptible to the certification scheme. At the same time, **foreign companies which are subject to the applicability of PIPL's extraterritoriality clause should also apply for the certification through a designated agent in China**. The key existing challenge to this is that the certification is currently done on a voluntary basis only: in practice, it remains to be seen how this will be enforced as it seems unlikely that foreign companies will apply voluntarily for certification.

In any case, the certification focuses on both the PI processor acting as exporter, and the offshore PI receiver. During the process, four key elements are reviewed:

- **Legally-binding agreement** signed by the PI exporter and the offshore receiver, which should clearly specify the: (i) identify of the PI exporter and offshore receiver; (ii) type and scope of PI to

Applying for certification for the cross-border transfer of personal information



Source: EU SME Centre

16 https://www.tc260.org.cn/upload/2022-06-24/1656064151109035148.pdf (accessed: 25 August 2022)

be transferred, and the purpose of the transfer; (iii) measures adopted to ensure the legitimate rights of PI owners; (iv) commitment of the overseas receiver to comply with Chinese laws and to accept supervision by the certification body; (v) responsible party within China; etc.[17]

- **Compliance of the two parties** in appointing a responsible officer and setting up a department in charge of protecting the personal information and the rights of owners;

- **Abiding by the same PI cross-border processing rules**

- **Personal information security impact assessment** that the PI exporter must carry out before the data transfer, in accordance with *GB/T 39335 – 2020 Information security technology - Guidance for personal information security impact assessment*.

The process is summarised in the graph on page 18.

It is noteworthy that, as of August 2022, the list of designated certification bodies for the certification has not yet been released. It is also unclear for how long the certification will be valid, once obtained. Hence, though looking promising and convenient for EU companies with a legal presence in China, in practice, this method of cross-border PI transfer is temporarily not an option as many details for implementation are still missing.

2.5 PENALTIES FOR NON-COMPLIANT CASES

Violating the obligations and requirements of cybersecurity, data security and personal information protection may trigger **administrative, civil, or even criminal liabilities** – depending on the specific circumstances and the impact on the rights of citizens, organisations, public interest, and national security. The CSL, DSL and PIPL include various articles with detailed penalties for different behaviours.[18] Under certain circumstances, not only the organisation but also responsible individuals may be punished.

To give an indication of the scale of monetary fines, 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. It is noteworthy that penalties may be drastically higher in case of multiple violations of different laws and regulations.[19] 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.

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.

17 Although not a formal requirement, it is recommended to redact the contract in line with the Standard Contract Provisions introduced in the previous section, even though the cross-border transfer is done through other methods such as certification or CAC security assessment: this will increase the chances of a positive outcome of the review.

18 For instance, Art. 59 to 75 of the CSL; Art. 44 to 52 of the DSL; Art. 66 to 71 of the PIPL.

19 For instance, in July 2022 CAC fined ride-hailing company Didi Chuxing USD 1.2 billion for severe violations of the CSL, DSL and PIPL, both domestically and through cross-border data, as it illegally collected nearly 12 million screenshots from users phones, 8.3 billion user clipboard and APPs information, 107 million pieces of facial recognition information, 153 million of location information, etc., posing serious threat to China's critical information infrastructure, data security, as well as national security. Didi's CEO and chairman were also fined. See: http://www.cac.gov.cn/2022-07/21/c_1660021534364976.htm (accessed: 25 August 2022).

III. TIPS AND FREQUENTLY ASKED QUESTIONS

3.1 COMPLIANCE TIPS FOR EU SMEs

There is no doubt that China's new governance framework for cybersecurity, data security and personal information protection brings a paradigm shift in the way EU companies have been operating their businesses and innovation activities in China. **Higher compliance requirements and costs** affect not only their current operations but especially their outlook in the country.

Each company is responding to such changes in different ways depending on their specific businesses, market share, risk-tolerance, integration within the Chinese ecosystem, as well as the integration of their China-based activities into global value chains.Size is also a key aspect: the previous sections of this report illustrated how **EU SMEs are relatively less affected** than large multinational corporations, especially when it comes to cross-border data transfers. This is because it is **less likely for SMEs to exceed the quantitative threshold triggering a security assessment, or to fall under the definition of important data**; at the same time, EU SMEs are traditionally less active in R&D or other data-intensive activities within China, with data flows mostly inbound rather than outbound.

Nevertheless, EU SMEs are still required to be compliant with the CSL, DSL and PIPL. The following actions may be taken to start assessing and ensuring compliance and thus prevent disruptions to their businesses in China.

Data mapping

*The first step should be to make a thorough and careful mapping of all the data and PI processing activities done in China – and abroad if subject to the extraterritorial reach of the DSL and PIPL. The mapping should also **clearly identify the amount and extent of outbound flows** of such data and PI.*

The mapping should also target the relationship of the company with its partners in China (e.g., suppliers, clients, but also IT and accounting service providers, etc.) to assess exposure and vulnerability to potential disruptions of data flows originating from their non-compliance.

Data assessment

*Based on the purpose, nature, amount of data and PI flows resulting from the mapping, the company should identify the corresponding requirements and security measures as indicated by the relevant laws, rules and standards – especially the Multi-Level Protection Scheme 2.0 and the grading system. At the same time, this assessment should also **clearly identify any data flows at risk of non-compliance in the future**, for instance increased data collection activities resulting from business growth, potentially exceeding the threshold for cross-border data transfer.*

Emergency plan

*Incidents such as network attacks or data breaches might happen even if security measures had been taken. The consequences on operations or fines from the authorities will depend on the effectiveness of the response: thus, it is fundamental to have a **sound contingency plan in place from the outset targeting different scenarios**.*

Crises and incidents are best dealt with in a time of peace and calm. This is anyway an obligation under the CSL, DSL and PIPL.

*The potential **impact of political factors** should always be considered to the extent possible.*

Review contracts/ policies

Even if SMEs might not be required to go through CAC's security assessment for transferring data, they are required to use Standard Contract Provisions issued by CAC or obtain a certification. EU SMEs should therefore review all their current contracts with Chinese partners and even employees, ***inform about changes and integrate amendments aligned as much as possible with the provisions****. The same applies to the privacy/cookie policies of websites.*

There is large evidence of EU SMEs in China already doing so.

Train personnel

In addition to appointing a dedicated resource overseeing all data and PI processing activities, it is vital that all the employees exposed to data flows – both in China and in the HQs in Europe – are ***regularly informed and trained*** *about the company's cybersecurity and data protection policies. The negligence of one individual employee might lead to non-compliance and severe consequences. SOPs for employees at all levels should be established on how to handle data processing and incidents. This is anyway an obligation under the DSL and PIPL.*

The above measures certainly take time and costs to implement. At the same time, these must be complemented by other actions aimed at **protecting intellectual property and trade secrets**: even if not explicitly stated, stricter review measures for cybersecurity (for obtaining access to the Chinese market for products or services) or cross-border data transfer (e.g. during the security assessment or certification process) in practice lead to **wider and deeper disclosure of sensitive business information**, potentially exacerbating an issue that has been long reported by EU business in China, particularly in the ICT, life sciences and automotive sectors.[20]

Yet, the **glass should not be necessarily seen as half-empty**: these new compliance requirements, although costly and imposed from the top, will objectively improve the security of a company's systems, reduce the risks of being infected by malware and enhance the capacity to deal with these incidents, thus avoiding damage and impact to operations.

Finally, EU SMEs must always keep in mind that China's governance regime for cybersecurity, data and personal information protection is far from being complete and is currently still in the shaping process. While writing this report, key regulations such as the *Network Data Security Regulations* and CAC's Standard Contract Provisions are still in the draft stage. This still leaves ample room for regulatory and enforcement changes or even ambiguity. **EU SMEs should therefore closely follow the developments in this field**, also by taking advantage of the various support initiatives funded by the EU.

The **EU SME Centre provides free-of-charge technical assistance to all EU SMEs** doing business in/ with China. We have a dedicated team of in-house and external experts ready to answer your questions on regulatory or business aspects, and also through one-to-one calls. EU SMEs may request this service through the **Ask-the-expert** section on our website, https://www.eusmecentre.org.cn/expert or by sending an email to info@eusmecentre.org.cn

20 See, for instance, the European Union Chamber of Commerce's Position Paper: https://www.europeanchamber.com.cn/en/publications-position-paper (accessed: 25 August 2022). For more information and free-of-charge technical assistance on IP and trade secrets, EU SMEs may contact the EU-funded project "China IP SME Helpdesk": https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/china-ipr-sme-helpdesk_en.

3.2 FREQUENTLY ASKED QUESTIONS

This section includes a list of **Frequently Asked Questions (FAQs)** specifically directed to EU SMEs doing business in/with China. Some of the FAQs were asked during a recent webinar organised by the EU SME Centre on the topic; [21] other FAQs were received by the EU SME Centre through the **Ask-the-expert** function; and some others are questions received by the EU SME Centre's partners, i.e. European embassies or business support organisations.

The answers are based on the experience, good practices and practical interpretation of relevant industry practitioners; **they do not constitute legal advice in any way and may be subject to different interpretations** by different practitioners.

At the same time, new changes, additions and adjustments of the legal framework are regularly introduced by relevant government administrations, including for specific sectors, clarifying existing doubts and introducing new requirements. Therefore, **the aim of the FAQs in this section is to provide general guidance** on the myriad of cases and peculiarities that may affect EU SMEs operating in/with China, reflecting the situation as of August 2022.

Do you have any other questions? Would you like to discuss in detail your case with one of our experts? Reach out to the **EU SME Centre's team of experts for free-of-charge assistance**!

https://www.eusmecentre.org.cn/expert
info@eusmecentre.org.cn

Compliance / applicability	*What are the most common cybersecurity and data compliance issues that foreign companies encounter in China?*
	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?
	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?
Important data	*How do I know if the data I generate in China from my business activities is important data?*
	Can I transfer important data to our company's HQs in Europe?
	My product collects data from the surrounding environment, such as cars' license plates or pictures of passers-by. Is this important data?
CIIOs	*Can foreign-invested companies be categorised as CII operators?*
Cross-border data transfer	*Can I transfer generic data to our company's HQs in Europe?*
	How should we interpret the 10 000 / 100 000 / 1 000 000 quantitative threshold for PI processing and cross-border transfer? Do these refer to single data entries or subjects?
	Our subsidiary in China collects business and personal information from operations there (e.g. clients, contracts, addresses, etc) and uploads them to our ERP system hosted in Europe – which is accessible to employees both in Europe and China. What should we do?

21 https://www.eusmecentre.org.cn/event/2022-05-24/cybersecurity-and-data-protection-china-compliance-challenges-and-tips.

Cross-border data transfer	*Our China-based subsidiary collects sensitive personal information of its employees (e.g., salary, addresses, health status, etc), then transfers them to Europe for HQs processing/records. Is this ok?*
	A company's European HQs directly entrust a China-based vendor for the processing and cross-border transfer of personal information collected in China, without any involvement of the company's China-based subsidiary. Is this compliant?
	There are different technical ways to process personal information. If data is anonymised, does it still count as personal information? Can it be transferred overseas?
	Are website cookies considered personal information? Can I transfer such information to our HQs in Europe for analytics and planning purposes?
	Our software, developed in the EU but used by Chinese users in China through licenses, automatically submits errors to the data centre in the EU for reporting and troubleshooting. Is this allowed?

a. What are the most common cybersecurity and data compliance issues that foreign companies encounter?

In general, there is still low awareness among foreign SMEs on the specific requirements and obligations to comply with China's cybersecurity, data, and personal information protection legal framework. A **common misperception is that SMEs think that their activities, the staff involved as well as hardware system used are so small in scale that they will pass unobserved or will be tolerated**. It is common to see such SMEs sending unprotected Excel worksheets abroad by email or instant messaging applications. Relatively few foreign-invested SMEs in China have very structured and localised IT systems; they usually mirror their systems and structure from abroad, without adjusting to the specific obligations stipulated by Chinese laws and regulations, for instance relating to PIPL's notice and consent. It is expected that many EU SMEs in China have not yet fully adapted to the new regulations.

While it will be harder for EU SMEs to reach the quantitative threshold that may trigger security assessment, they are nonetheless **still required to be fully compliant with Chinese laws and regulations**; failure to do so may result in fines or more severe consequences.

b. 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?

As seen in section 2.1 of this report, both the DSL and PIPL have extraterritorial reach. Therefore, 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.[22] 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.

Yet, without the direct involvement of a China-based legal entity acting as an 'exporter' of the data or personal information, it will be challenging for Chinese authorities to **monitor non-compliant cases and enforce relevant action**. However, because all entities subject to PIPL must provide a data subject response mechanism (e.g., answering users' requests on their data), it is likely that that foreign entities without presence in China would be reported by their China-based users for lack of compliance with the law. Potentially feasible repercussions for the EU SME could involve blocking the accessibility of its website from within the Chinese territory, the impossibility for the SME to pass security assessments as an offshore receiver in future transactions with China-based data exporters, or even blacklisting in severe cases. In any case, the situation is under constant development; relevant EU SMEs are advised to closely monitor the situation.

22 Indeed, as seen in section 2.4 of this report, the *Certification Requirements for Cross-border Transfer of Personal Information* issued by TC260 stipulate that foreign companies not in China will also need to apply for the certification through a domestic brand or designated agent, carrying out the security impact assessment and be reviewed by the Chinese certification body.

c. 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?

As indicated in the previous FAQ, 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 – most likely a security assessment with CAC as it is expected to exceed the threshold of PI processed. 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; on the positive side, in general, **compliance to GDPR makes it relatively less troublesome to adapt to PIPL obligations**.

d. How do I know if the data I generate in China from my business activities is important data?

As seen in section 2.2, important data is data that, if tampered with, leaked, compromised, or illegally acquired or used, may cause harm to national security or public interest. If at least one of the conditions indicated by the draft guidelines issued by TC260 is present (summarised in the box below), then the data would be considered important data – whose export may be allowed only after a prior security assessment is conducted and passed with CAC.

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

As seen in section 2.4 of this report, 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).

*A detailed translation of TC260's guidelines is included in Annex 1 of this report. To summarise, the **following types of data are <u>not</u> to be considered important data:***

- *Personal information – although data derived from a large amount of personal information may still be considered important data*
- *Data that are only important or sensitive to the organisation itself*
- *Trade secrets protected as such by companies*
- *Business information provided to Chinese clients who are not CII operators*
- *Data as well as technical information not involving items under export control, such as dual-use items, nuclear-related*
- *Data not involving undisclosed information obtained from/on government agencies, military organisations or targets*
- *Data not involving China's national resources, environment, spatial information, and population*
- *Data not involving critical strategic materials, components and relevant supply chains*

Additional requirements and obligations might exist for specific industries. For instance, scientific data produced under any government-funded project in China, as well as any genetics data, must be stored within China and cannot be published on international journals without prior approval, and must be shared with Chinese collaborators. Finally, further restrictions or bans exist for Chinese entities (including subsidiaries of foreign companies) that want to transfer intellectual property rights overseas – based on a MOST-MOFCOM catalogue.[23]

f. My product collects data from the surrounding environment, such as cars' license plates or pictures of passers-by. Is this important data?

As indicated in section 2.2, any information that may be used to identify natural persons or their activities in China is considered personal information. This includes information such as biometric information of individuals, as well as license plates of cars passing by.

Elements such as population and environment are among the key factors to consider when determining the importance of data. Although personal information is generally not considered important data, however, statistical data and derived data generated

23 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 (accessed: 25 August 2022)

based on large-scale personal information may be regarded as important data; even if not, considering the size of China's population (i.e., the number of people or cars that could be at any given time in a certain place in any Chinese city), the processor of such personal information would probably be considered a large-scale PI processor (i.e., entity processing the personal information of more than 1 million individuals), and thus be subject to the same localised storage and security assessment requirements as processors of important data.

Yet, if such PI is anonymised (see relevant FAQ below), for instance if facial traits of passers-by are pixelated, geographical locations removed, building names unspecified, etc., the situation might be different. A careful legal assessment will be needed for each specific case.

g. Can foreign-invested companies be categorised as CII operators?

Currently, China's cybersecurity laws and regulations **do not have explicit provisions excluding foreign-invested companies to be categorised as CII operators**. Hence, in principle, foreign-invested companies operating in China could be categorised as CII operators; yet, it is not very realistic for EU SMEs.

Clearly stipulated by relevant laws and regulations, is that relevant government bodies will be responsible for network protection in their areas of competence, hence they will also be responsible for stipulating a detailed list of CIIs and their operators in their areas. Those entities ending up in such lists will be formally notified by the relevant government body: if a company has not received any formal notification from its supervisory body, then it most likely is not considered as CII operator and thus does not need to comply with the relevant requirements and obligations.

> ***Example**: providing a product or technology to sectors such as energy or environment (e.g. a digital monitoring device or a water pump), does not make the manufacturer a CII operator. By contrast, the Chinese client using the product or technology (e.g. a power plant operator or manager of the water supply network) would more likely be categorised as CII operator – with specific obligations on ensuring the network and data safety and protection of the product/ technology used.*

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

Yes. As illustrated in section 2.4, 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 (see the Multi-Level Protection Scheme in Annex 2), 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.

i. 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?

Currently, 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.

j. Our subsidiary in China collects business and personal information from operations there (e.g. clients, contracts, addresses, etc) and uploads them to our ERP system hosted in Europe – which is accessible to employees both in Europe and China. What should we do?

The answer depends on the nature and amount of information collected. If:

- the data is not considered important data
- and at the same time, if the subsidiary in China is not a CII operator or a large-scale PI processor (processing PI of more than 1 million individuals)

- and if the personal information to be uploaded in the overseas ERP system does not exceed the annual threshold (100 000 individuals, or 10 000 sensitive personal information)

Then, the company does not need to apply for security assessment before uploading the information on its overseas-hosted ERP system; but it must use the Standard Contract Provisions issued by CAC or obtain a certification by a designated body. In practice, there is evidence of EU SMEs in China which have already **revised all existing contracts with their business partners in China**, by adding the standard contract provisions (see section 2.4), completing a self-assessment, and filing the two documents with provincial-level CAC.

If, however, at least one of the three conditions above is not met, then security assessment with CAC will be needed before the information may be uploaded in the ERP system.

k. Our China-based subsidiary collects sensitive personal information of its employees (e.g., salary, addresses, health status, etc), then transfers them to Europe for HQs processing/records. Is this ok?

Personal information and sensitive personal information collected in China (e.g. the employees of a subsidiary) fall fully under the scope of the PIPL. Therefore **China-based subsidiaries must fully comply with the relevant obligations** for the process, use, and cross-border transfer of such information: a security assessment must be completed, Standard Contract Provisions used, or a certification obtained, depending on whether the quantitative threshold of PI is exceeded. As indicated in section 2.4, it seems that the certification process is more suitable for cross-border transfers among entities belonging to the same business group. In any case, the first steps would be to limit the transfer to information necessary for performance of labour contracts to avoid seeking for consent, and inform all employees about the cross-border PI processing activities by including the cross-border transfer in the Privacy Notice.

In practice, however, this issue is a bigger concern for large multinational corporations employing thousands of individuals rather than for SMEs.

l. A company's European HQs directly entrust a China-based vendor for the processing and cross-border transfer of personal information of individuals located in China, without any involvement of the company's China-based subsidiary. Is this compliant?

Yes, as long as both the European HQs and the entrusted China-based vendor fully comply with the obligations and requirements of the CSL, DSL, PIPL and other regulations. Yet, it is suggested that the HQs start to involve their China-based subsidiary in the process, to supervise and ensure the vendor's full compliance, and formulate emergency response plans in case of incidents. Furthermore, in such cases, the European HQs are required to appoint a representative in China in line with PIPL's extraterritorial reach.

m. There are different technical ways to process personal information. If data is anonymised, does it still count as personal information? Can it be transferred overseas?

Art. 4 of the PIPL stipulates that personal information refers to a variety of information that can be used to identify natural persons and are recorded electronically or by other means – **excluding information processed anonymously**. Anonymised information specifically indicates personal information that, after processing, cannot identify specific natural persons, and that at the same time cannot be restored to its original form; hence, **it does not apply to de-identification**.

Therefore, if a China-based PI processor makes a full degree of anonymisation without the possibility of restoring the original state of the information, then it does not need to follow the DSL and PIPL requirements for cross-border transfer. If, however, the anonymisation is only partial, or it can be annulled so that the original state of the information can be restored, then the China-based PI processor will still need to comply with relevant provisions.

At the same time, it must be kept in mind that, even with full anonymisation, such information might still be classified as important data – especially if the data involve population, genetics, items under export control, etc. In these cases, a prior security assessment with CAC will be needed before transferring such data. Companies are therefore recommended to make a comprehensive assessment of the degree of anonymisation of their data, as well as its nature.

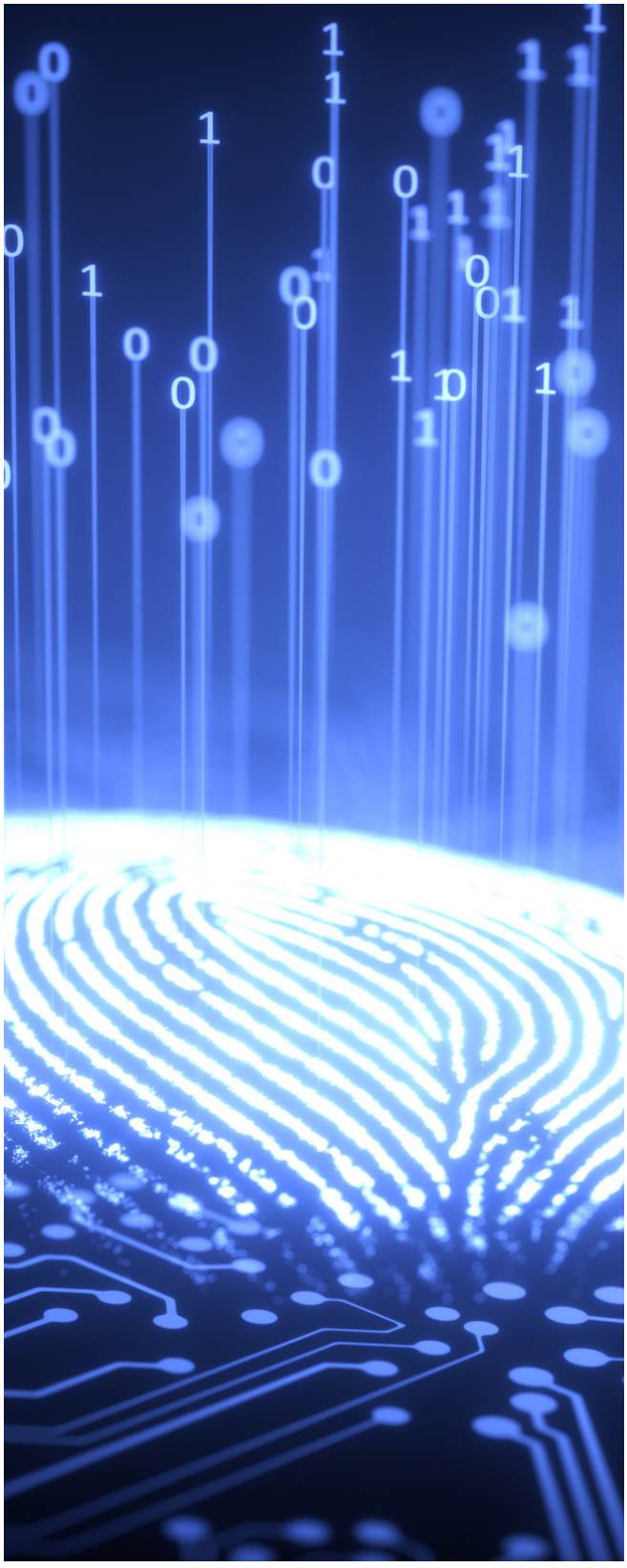
n. Are website cookies considered personal information? Can I transfer such information to our HQs in Europe for analytics and planning purposes?

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 indicated in section 2.3, 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.

o. Our software, developed in the EU but used by Chinese users in China through licenses, automatically submits errors to the data centre in the EU for reporting and troubleshooting. Is this allowed?

This type of activity falls within the scope of cross-border data transfer, therefore the corresponding procedures indicated in section 2.4 must be followed according to the different requirements for data and PI. If the data submitted does not belong to important data, the processor is not a large-scale PI processor (1 million individuals), and the personal information to be transferred does not exceed the cumulative annual threshold (100 000 individuals or 10 000 sensitive personal information), then such operation is allowed provided that the principles and obligations for data/personal information collection and the legitimate rights of PI owners are fully respected (e.g. full information disclosed to the user, voluntary consent to be explicitly given through a pop-up window, anonymisation, etc), and that Standard Contract Provisions are used or certification obtained as this still constitutes a cross-border transfer.

However, each case may be significantly different and therefore careful legal analysis and assessment are recommended.



IV. ANNEXES

4.1 ANNEX 1 – GUIDELINES FOR THE IDENTIFICATION OF IMPORTANT DATA

If **at least one of the below principles or factors to consider applies, then the data would be considered important data**, thus triggering specific obligations for its localised storage, protection and security assessment in case of cross-border transfer.

Detailed guidelines are in the process of being formulated by relevant competent authorities and provincial-level authorities for the identification of important data in their specific sectors and regions. For instance, the China Communications Standards Association in 2021 issued the sector standard *YD/T 3867-2021 Important Data Identification Guide for Basic Telecom Enterprises*; more will follow.

	Principles to respect	Factors to consider
IDENTIFICATION OF IMPORTANT DATA	**Focus on impact on security**: important data shall be identified from the perspective of national security, economic operations, social stability, public health and safety. ***Data that are only important or sensitive to the organisation itself are not important data***, e.g. data on internal management of the enterprise.	Data reflecting **national strategic reserves and emergency mobilisation capacities** belongs to important data, e.g., data on production and reserve capacities of strategic materials
	Define the focus of protection: based on data classification, the focus of security and protection should be clearly defined, so that both generic data and important data may flow smoothly on the premise that security and protection requirements are met.	Data supporting **CII operations or industrial production in key fields** belongs to important data, e.g., data directly supporting industries where CIIs are located, as well as data generated through core business operations or industrial production in key fields
	Cohesion with existing provisions: the existing local management regulations and industry characteristics shall be fully considered, and closely link up with the relevant data management policies, standards and norms that have been formulated and implemented by local government departments.	Data reflecting the **network security of CIIs** and which can be used to implement **network attacks** belongs to important data – e.g., data reflecting CII network security scheme, system configuration information, core software and hardware design information, system topology, emergency plans, etc.
	Comprehensive risk management: the risks of tampering, destruction, disclosure, illegal acquisition and illegal use of data shall be fully considered based on different factors, thus identifying important data from the perspectives of confidentiality, integrity, availability, authenticity, accuracy.	Data related to **export control items** belongs to important data – e.g., information describing the design principle, technological process or production methods of export control items, or source code, integrated circuit layout, technical scheme, important parameters, experimental data and test reports.[24]
	Combination of quantitative and qualitative aspects: important data shall be identified both quantitatively and qualitatively; relevant methods shall accordingly be adopted for specific data types and characteristics.	Data that may be used by other countries or organisations to launch **military attacks against China** belongs to important data – e.g., geographic information that meets certain precision requirements.

24 In addition to regulations for data activities and transfer, China has also enacted various laws and regulations on **export control**. For instance, The 2020 *Export Control Law* stipulates that goods, technologies, services and items relating to the maintenance of national security and national interests may be restricted or prohibited from export – temporarily or permanently; this includes data such as technical information, thus covering research, joint research or technology sales provided as a service by a Chinese domestic entity to foreign entities. Detailed lists of controlled items are produced by MOFCOM. http://www.gov.cn/xinwen/2020-10/18/content_5552119.htm (accessed: 25 August 2022).

	Principles to respect	Factors to consider
IDENTIFICATION OF IMPORTANT DATA	**Dynamic identification and review**: the identification of important data shall take into account factors such as changes in the purpose of data use, sharing modalities, importance, etc., and thus regularly reviewed and reassessed.	Data reflecting the **physical security of key targets**, important places or the location of undisclosed geographical targets which may be used by terrorists and criminals for destruction purposes belongs to important data – e.g., construction drawings, data on the internal structures of key security units, major production enterprises, important national assets (railways, oil pipelines), as well as undisclosed special roads, undisclosed airports, etc.
		Data which may be used to **disrupt the supply chains of critical equipment and system components** through network attacks and threats belongs to important data – e.g., lists of important customers, the procurement of products and services by operators of undisclosed critical information, and undisclosed major vulnerabilities.
		Basic data reflecting **population health, physiological status, ethnic characteristics and genetic information** belongs to important data – e.g., census data, human genetic resources, and original data of gene sequencing.
		Basic data on **natural resources and environment** belongs to important data – e.g., undisclosed hydrological information, hydrological observation data, meteorological observation data and environmental protection monitoring data.
		Data relating to **sci-tech strengths and affecting international competitiveness** belongs to important data – e.g., data describing IP rights related to national defence and national security.
		Data on the **production, use or transaction of sensitive items and equipment which may be sanctioned by foreign governments** belongs to important data – e.g., financial transaction data of key enterprises, manufacturing information of important equipment, and use of important equipment in national major projects.
		Confidential information when providing services to government agencies, military enterprises and other sensitive and important organisations belong to important data – e.g., vehicle use information of military enterprises.
		Undisclosed government data, work secrets, intelligence data and law enforcement judicial data belong to important data – e.g., undisclosed statistics.
		Other data that may affect national political, territorial, military, economic, cultural, social, scientific and technological, ecological, resources, nuclear facilities, overseas interests, biological, space, polar, deep-sea security, etc.

4.2 ANNEX 2 – CLASSIFICATION AND GRADING OF NETWORKS AND DATA

China has issued a series of standards further dividing network systems and data into different security levels, based on their importance and the impact that their infringement would have on citizens, organisations, public interest or national security. Different security levels correspond to different security requirements and obligations for their operators – domestic and foreign companies alike. These standards are: the cyber **Multi-Level Protection Scheme 2.0 for networks**, and the **Classification and Grading for Data**.

Cyber Multi-Level Protection Scheme 2.0 for networks

Consistent with the CSL and DSL, network systems must be protected by their operators based on a series of standards (GB/T 22239-2019, GB/T 25070-2019, GB/T 28448-2019), commonly known as the cyber **Multi-Level Protection Scheme (MLPS) 2.0** — as it was last updated in 2019 from a previous version.

The MLPS 2.0 outlines five different levels of network security protection, based on (i) the importance of the network, (ii) the object of infringement – i.e. citizens/organisations, social order/public interest, and national security, and (iii) the impact of infringement – i.e. general, serious or severe. The higher the level, the stricter the security requirements will be for the operators. Government systems and facilities are usually associated with Level 4 and 5, CIIs and systems on which important data is processed with Level 3, **while foreign-invested SMEs processing generic data are usually associated with level 1 or more rarely with 2.**

It is noteworthy that, according to the MLPS 2.0, each network operator is responsible to engage a qualified testing agency in China to determine the security level of its network and assess the effectiveness of the corresponding protection measures adopted. Operators of Level 2 (or above) networks will need to file the assessment certificate with the provincial-level public security department, while those of Level 1 are not required to do such filing. [25]

	Impact on citizens, organisations			Impact on social order, public interest			Impact on national security		
	General	Serious	Severe	General	Serious	Severe	General	Serious	Severe
Basic networks 一般网络	1	2	/	2	/	/	/	/	/
Important networks 重要网络	/	/	3	/	3	/	3	/	/
Very important networks 特别、极其重要网络	/	/	/	/	/	4	/	4	5

25 For more details on the requirements, procedures, as well as costs of MLPS filing, find a relevant article published by AppInChina: https://www.appinchina.co/what-is-an-mlps-filing-and-who-needs-one (accessed: 25 August 2022). AppInChina also participated to a EU SME Centre webinar in April 2022 about the export of software as a service from Europe to China, see: https://www.eusmecentre.org.cn/event/2022-04-07/how-sell-software-china.

Classification and grading system for data

Similar to the MLPS for network systems, a **classification and grading system** is also being established for data – as indicated by the draft *Network Data Security Regulations* released by CAC in November 2021 (Art. 5). Based on the data's importance and impact on individuals/organisations, public interest, and national security, processors will need to adopt different measures to ensure data security and integrity.

More details are provided by the standard *Network Security Standards Practice: Guidelines for Network Data Classification and Grading* formulated by TC260.[26] Four levels ('grades') are indicated for three types ('classes') of data, namely core data, important data, and generic data. The higher the level, the higher its infringement impact and the stricter the security requirements will be for the operators. Generic data, if leaked or damaged, will not have any impact on public interest or national security, but only different degrees of impact on the rights of citizens and organisations; by contrast, important data will have light to normal impact on national security and public interest, but no impact on the rights of citizens and organisations; finally, core data will have a serious impact on national security and public interests.

It must be noted that, at the time of writing this report, the implementation of the above standard is not yet mandatory – only recommended. Detailed obligations and rules will be clarified with the final version of the *Network Data Security Regulations*, expected by the end of 2022.

	Objects and impact of infringement			
	National security	**Public interest**	**Rights of individuals**	**Rights of organisations**
Core data	Normal to generic impact	Severe impact	No impact	
Important data	Light impact	Light to generic impact	No impact	
Generic data	No impact		No impact, light impact, generic impact, or severe impact	

26 https://www.tc260.org.cn/upload/2021-12-31/1640948142376022576.pdf (accessed: 25 August 2022).

About the EU SME Centre

The EU SME Centre helps European SMEs get ready for China by providing them with a range of information, advice, training and support services.

To find out more, visit: www.eusmecentre.org.cn

Consortium partners:

Camera di Commercio Italiana in Cina
中国意大利商会
China-Italy Chamber of Commerce

European Union Chamber of Commerce in China
中 国 欧 盟 商 会

ICCF ITALY CHINA COUNCIL FOUNDATION

spi Sociedade Portuguesa de Inovação

Associated partners:

TRADE PROMOTION EUROPE
One voice for European trade promotion

EU-China Business Association
欧盟中国贸易协会

Do you have a question about doing business in China?

Ask one of our in-house experts and receive practical and confidential advice within seven working days. We can provide information and advice relating to business development, market access, legal issues, and human resources.

To submit your enquiries directly to our experts go to **Ask-the-Expert**: www.eusmecentre.org.cn/expert, or contact us at info@eusmecentre.org.cn

Further reading...

The EU SME Centre has nearly 200 **reports, guidelines** and case studies in its Knowledge Centre, the following may be relevant to you:

- *Personal Information and Cybersecurity Protection in China (April 2022): https://www.eusmecentre.org.cn/guideline/personal-information-and-cybersecurity-protection-china*

We have also available **recordings of previous webinars** in this field:

- *Data and cybersecurity in China: compliance, challenges and tips (May 2022): https://www.eusmecentre.org.cn/event/2022-05-24/cybersecurity-and-data-protection-china-compliance-challenges-and-tips*
- *PIPL practical guide in retail and marketing trends (Jan 2022): https://www.eusmecentre.org.cn/event/2022-01-21/pipl-practical-guide-retail-and-china-marketing-trends-2022*

Funded by the European Union