国际数据跨境规则系列

Series on International Data Cross-Border Rules

中国数据出境实务实操白皮书

White Paper on Chinese Practice of Outbound Data Transfers

实务问答与实操演练

Operational Q&As + Practical Exercises

段和段律師事務所
DUAN & DUAN

二零二四年一月

January 2024

前 言
Preface

作为数据要素流动的主要国家之一，中国已经就数据跨境流动建立了完善的合规监管机制。三条数据出境的合规路径——安全评估、标准合同备案、个人信息保护认证，现均已正式落地实施，各省市陆续均有通过案例出台，行业遍布生物医药、汽车制造、跨境电商、企业征信等行业。

As one of the main countries in the flow of data elements, China has already established a comprehensive compliance regulatory mechanism for cross-border data flows. Three paths for outbound data transfers—security assessment, standard contract filing, and personal information protection certification—have all been formally implemented, with various provinces and cities introducing cases across industries such as biopharmaceuticals, automotive manufacturing, cross-border e-commerce, and corporate credit reporting.

与此同时，中国也在积极制定推动相关“**减负**”政策，进一步为企业降低合规成本。如2023 年 9 月 28 日征求意见的《规范和促进数据跨境流动规定》，明确罗列了数据出境的豁免情形；又如 12 月出台的《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》，针对内地与香港之间的个人信息流动的合规要求进行了简化。

At the same time, China is also actively formulating and promoting relevant “burden reduction” policies to further reduce compliance costs for enterprises. For example, the "Provisions on Regulating and Promoting Cross-border Flow of Data (Exposure Draft)" issued on 28 September 2023, clearly listed the exemptions for data outbound tranfers; Similarly, the “Implementation Guidelines on the Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)”, issued in December 2023, simplifies the compliance requirements for the flow of personal information between the Mainland and Hong Kong.

选择哪种路径出境、谁来申请数据出境、如何实现合规出境，是绝大多数外资企业及跨国集团公司等主体的困惑所在。为此，我们从企业实际业务场景出发，针对企业关注的核心

问题梳理形成本白皮书（实务问答+实操演练），希望能够帮助企业明晰合规路径，实现数据的有序流动。

Choosing the right path for export, determining who applies for data export, and figuring out how to achieve compliant data export are major challenges for most foreign-owned enterprises and multinational corporations. For this reason, we wrote this white paper, starting from the actual business scenarios of enterprises, and combing through the core issues of enterprises' concern to form Operational Q&As and Practical Exercises. We hope this will help enterprises to clarify the compliance path of outbound data transfer and achieve the orderly flow of data.

面对数据出境路径的选择，我们分别以三条路径为轴，逐一拎出各通路上将面临的问题并予以分析，总结出 30 个实务问题+10 个实操案例，采用一问一答的方式，辅以实操演练，通过剖析解读法规政策、挖掘数据出境常见场景，为拟出境企业选择出境路径提供指导思路，为强监管下的数据出境提供应对之道。

In the face of the choice of outbound data transfer paths, we respectively take three paths as the axis, addressing the issues and conducting analyses for each path one by one. We have summarized 30 operational questions along with 10 real cases, presented in a Q&A format supplemented by practical exercises. By analyzing and interpreting the regulations and policies, as well as exploring common scenarios in outbound data transfers, we provide guidance for enterprises on choice of the right paths, and help them to find a way out of the strong regulation.

目录
Contents

— 概　览 (Overview) —

一、中国数据出境路径透视

I. Pivot View of China's Outbound Data Transfer Paths

(一) 路径起源

(I) Origins of Paths

数据跨境流动是全球化数字经济的必然，数据主权、数据安全以及个人信息保护也是全球监管的共识。

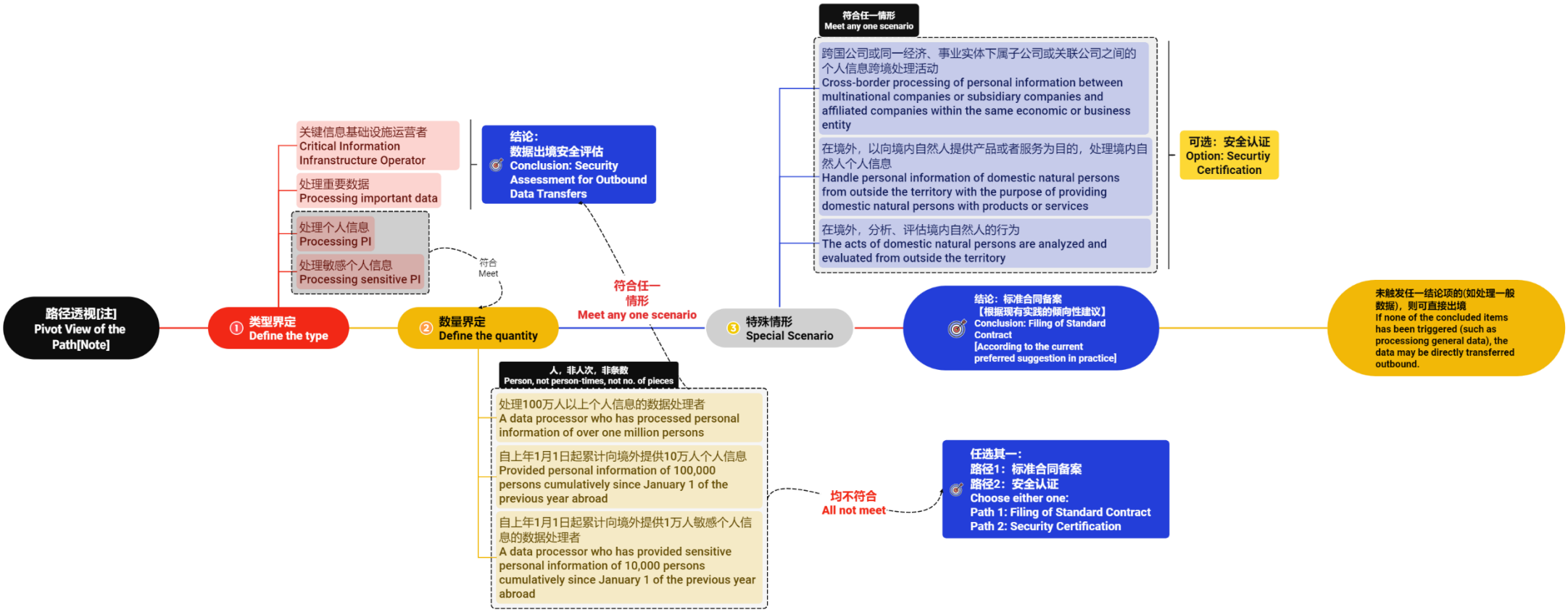
The cross-border flow of data is an inevitable part of the globalized digital economy, and there is consensus that the protection of data sovereignty, data security, and personal information protection are subject to global regulation.

我国目前法律就数据出境提供了三条通路，即：数据出境安全评估、个人信息出境标准合同备案（或称“标准合同备案”）、个人信息跨境处理活动安全认证（或称“个人信息保护认证”）。三者均来源于《个人信息保护法》第 38 条第 1 款的规定，个人信息处理者因业务等需要，确需向境外提供个人信息的，应当具备下列条件之一：（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；（三）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；（四）法律、行政法规或者国家网信部门规定的其他条件。

China's current laws provide three paths for outbound data transfers, namely: security assessment for outbound data transfers, the filing of the Standard Contract for outbound transfer of personal information (or "**SC Filing**"), and security certification for cross-border processing activities of personal information (or "**Personal Information Protection Certification, PIPC**"). All three are derived from Article 38, Paragraph 1 of the Personal Information Protection Law, which provides that where a PIP genuinely needs to provide personal information outside the territory of the People's Republic of China due to business or other needs, it shall meet any of the following conditions: (I) to have passed the security assessment organized by the Cyberspace Administration of China in accordance with the provisions of Article 40 thereof; (II) to have obtained a Personal Information Protection Certification issued by a specialized agency in accordance with the regulations of the Cyberspace Administration of China; (III) to have entered into a contract with an oversea recipient under the standard contract formulated by the Cyberspace Administration of China, specifying the rights and obligations of both parties; or (IV) to meet other conditions prescribed by laws, administrative regulations or the Cyberspace Administration of China.

(二) 路径选择

(II) Path Selection



注：特别地，针对注册在粤港澳大湾区内地部分/香港特别行政区的个人信息处理者及接收方，在粤港澳大湾区内地部分与香港特别行政区之间的个人信息跨境流动，不含重要数据的，可以选择标准合同备案。

In particular, for PI processors and recipients registered in the Mainland part of the Guangdong-Hong Kong-Macao Greater Bay Area/Hong Kong SAR, for cross-border flow of personal data between the Mainland part of the Guangdong-Hong Kong-Macao Greater Bay Area and the Hong Kong SAR that does not contain important data, the option of filing of standard contract is available.

(三) 路径豁免（或有）

(III) Path Exemptions (if any)

与此同时，为进一步降低企业在数据跨境传输方面的合规成本，国家互联网信息办公室在 2023 年 9 月 28 日出台了《规范和促进数据跨境流动规定（征求意见稿）》（下称“《征求意见稿》”），意图为数据要素跨境流通“减负”。该《征求意见稿》主要明确了以下两点：

Meanwhile, in order to further reduce the compliance cost of enterprises in cross-border data transfer, the Cyberspace Administration of China issued the "Provisions on Regulating and Promoting Cross-border Flow of Data (Exposure Draft)" (the “Exposure Draft”) on 28 September 2023, with the intention of reducing the burden of cross-border flow of data elements. The Exposure Draft clarifies the following two main points:

1. 【**新增豁免情形**】符合以下情形之一的，不需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证：

   【**Exemptions**】Under any of the following circumstances, it is not required to apply for security assessment for outbound data transfers, the SC Filing, and PIPC：

- 国际贸易、学术合作、跨国生产制造和市场营销等活动中产生的数据出境，不包含个人信息或者重要数据的；

  where data outbound transfer arising from international trade, academic cooperation, cross-border production and manufacturing, marketing activities, and others, excluding the transfer of personal information or important data;

- 不是在境内收集产生的个人信息向境外提供；

  providing personal information not collected in China to locations outside China;

- 为订立、履行个人作为一方当事人的合同所必需，如跨境购物、跨境汇款、机票酒店预订、签证办理等，必须向境外提供个人信息的；

  where the personal information must be provided abroad, as it is necessary for the conclusion and performance of a contract to which the individual is a party, such as cross-border shopping, cross-border remittance, air tickets and hotel booking, visa processing, etc.

- 按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理，必须向境外提供内部员工个人信息的；

  for human resources management in accordance with the labor regulations and rules formulated in accordance with the law and collective contracts concluded in accordance with the law, it is necessary to provide abroad the personal information of internal employees;

- 紧急情况下为保护自然人的生命健康和财产安全等，必须向境外提供个人信息的；

  where personal information has to be provided overseas to protect the life, health, and property safety of natural persons in an emergency; and

- 预计一年内向境外提供不满 1 万人个人信息的。

  where the PIP is expected to provide personal information of less than 10,000 individuals to locations outside China within one year.

2. 【**鼓励创新试点**】自由贸易试验区可自行制定本自贸区需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单（以下简称负面清单），负面清单外数据出境，可以不申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

   【**Encouraging Innovative Pilots**】Pilot free trade zones may, on their own, formulate lists of data that need to be included in the scope of administration of security assessment for the data to be provided abroad, standard contracts for outbound provision of personal information, and certification for personal information protection (the "Negative List"), and data outbound transfer activities outside the Negative List may be carried out without applying for security assessment for outbound data transfers, the SC Filing, and PIPC.

目前该《征求意见稿》尚未正式出台，但已明确释放出促进数据跨境自由流动的强烈信号。相信数据跨境有序合规自由流通的机制将很快建立起来。

The Exposure Draft has not yet been formally issued, but it has clearly released a strong signal to promote the free flow of data outbound transfers. It is believed that a mechanism for the orderly and compliant free flow of data across borders will soon be established.

— 数据出境实务 30 问答 (30 Q&As) —

二、中国数据出境实务问答

II、Q&A on Chinese Practices of Outbound Data Transfers

(一) 数据出境安全评估 10 问

(I) 10 Questions on Security Assessment for Outbound Data Transfers

Q1: 什么情形必须启动数据出境安全评估？

Under what circumstances must security assessment for outbound data transfers be conducted?

A1: 具备以下情形之一时，必须启动数据出境安全评估：

A security assessment for outbound data transfers must be conducted when one of the following circumstances arises:

(1) 数据处理者向境外提供重要数据；

where a data processor provides important data abroad;

(2) 关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；

where a key information infrastructure operator or a PIP of the data of more than one million people provides abroad personal information;

(3) 自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；或者

where a PIP has provided abroad personal information of 100,000 people or sensitive personal information of 10,000 people in total since January 1 of the previous year; or

(4) 国家网信部门规定的其他需要申报数据出境安全评估的情形。[1]

[1] 《数据出境安全评估办法》（国家互联网信息办公室，国家互联网信息办公室令第 11 号，

Other circumstances prescribed by the Cyberspace Administration of China for which declaration for security assessment for outbound data transfers is required.

特别地，该境外包含香港特别行政区、澳门特别行政区以及台湾地区。

In particular, this territory includes the Hong Kong Special Administrative Region, the Macao Special Administrative Region, and Taiwan.

Q2: 数据出境行为具体包含哪些？

What constitutes an act of outbound data transfer?

A2: 数据出境行为包括向境外提供或允许境外访问境内数据，具体包括以下三种情形：

Acts of data outbound transfers include providing or allowing access to data within the territory from outside the territory, specifically including the following three situations:

(1) 数据处理者将在境内运营中收集和产生的数据传输、存储至境外；

The data processor transfers and stores the data collected and generated in its operations within the territory abroad;

(2) 数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出；

Data collected and generated by data processors are stored in the territory and can be queried, accessed, downloaded, or exported by institutions, organizations, or individuals abroad;

(3) 国家网信办规定的其他数据出境行为。[2]

2022.07.07 发布，2022.09.01 实施）第 4 条规定。
Article 4, Measures for the Security Assessment of Outbound Data Transfer (Cyberspace Administration of China, Order No.11 of the Cyberspace Administration of China, issued on 7 July 2022, effective from 1 September 2022)

[2] 《数据出境安全评估申报指南（第一版）》（国家互联网信息办公室，2022.08.31 发布，2022.08.31 实施）“一、适用范围”规定。
“1. Scope of Application” of Guidelines for the Application for Security Assessment for Outbound Data Transfers (First Edition) (Cyberspace Administration of China, issued on 31 August 2022, effective from 31 August 2022)

Other acts of outbound data transfers stipulated by the Cyberspace Administration of China.

◆ 实操演练 1

Practical Exercise 1

Q：跨境电商平台有许多商家，如何申报数据出境安全评估？跨境电商场景下平台方与品牌方，谁来发起安全评估？

Q: Cross-border e-commerce platforms have many merchants, how to declare security assessment for outbound data transfers? In the context of cross-border e-commerce between the platforms and the brands, who will conduct the security assessment?

A：需要区分场景。根据数据实际由平台还是品牌方传输出境，品牌方自行传输出境的场景下，品牌方申报；平台传输出境的场景下，平台统一申报。

A: There is a need to distinguish the scenarios. It is based on whether the data are actually transmitted by the platforms or the brands, if the brands transmit the data outside the territory of the People's Republic of China themselves, the brands should make the declaration. If the platforms transmit the data outside the territory of the People's Republic of China, the platform should make a consolidated declaration.

◆ 实操演练 1 延伸

Variation of Practical Exercise 1

境内 A 公司员工在境外出差，将 A 公司业务经营中处理的重要数据通过硬盘方式提供给境外 B 公司。

An employee of Company A within the territory is on business trip outside the territory and provides important data processed by Company A in business operation to Company B abroad via a hard drive.

Q：该 A 公司是否应当启动数据出境安全评估？

Q: Should Company A conduct a security assessment for outbound data transfers?

A：通过硬盘传输亦属于数据出境，应当事前通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

A: Transferring data via a hard drive also constitutes outbound data transfers, so Company A should declare a security assessment for outbound data transfers to the national cyberspace administration department via the provincial-level cyberspace administration department in advance.

Q3: 如何识别“重要数据”？

How to identify "important data"?

A3: 重要数据，是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。[3]

Important data refers to data that may jeopardize national security, economic operation, social stability, public health, safety, etc., if it is tampered with, damaged, leaked, illegally accessed, or illegally utilized, etc.

在重要数据识别时，应当优先参考所属行业、领域、地区数据安全管理相关规定（例如汽车数据对应的《汽车数据安全管理若干规定（试行）》（下称“《汽车数据规定》”），其次可参考《网络数据安全管理条例（征求意见稿）》中相关定义：

When identifying important data, priority should be given to taking reference from relevant regulations on data security management of the industry, field, and region to which it belongs (e.g., automobile data corresponds to the "Several Provisions on Automotive Data Security Management (for Trial Implementation)", "Provisions on Automobile Data"), and to a lesser extent, to the relevant definitions in the "Regulations for the Administration of Network Data Security (Exposure Draft) ":

(1) 未公开的政务数据、工作秘密、情报数据和执法司法数据；

Unpublished government data, working secrets, intelligence data, and law enforcement and judicial data;

(2) 重点行业和领域安全生产、运行的数据、关键系统组件、设备供应链数据；

Data on safe production and operation of key industries and fields, key system components, and equipment supply chain data;

[3] 《数据出境安全评估办法》（国家互联网信息办公室，国家互联网信息办公室令第 11 号，2022.07.07 发布，2022.09.01 实施）第 19 条规定。
Article 19, Measures for the Security Assessment of Outbound Data Transfers (Order No. 11 of the Cyberspace Administration of China, issued on 7 July 2022, effective from 1 September 2022)

(3) 达到国家有关部门规定规模或者精度的基因、地理、矿产、气象等国家基础数据；

National basic data such as genetics, geography, minerals, meteorology, etc. that have reached the scale or precision specified by the relevant state departments;

(4) 影响关键信息基础设施安全稳定运行的数据，国防设施、军事管理区、国防科研生产单位等重要敏感区域的地理位置、安保情况等数据；

Data affecting the safe and stable operation of critical information infrastructures, the geographic location and security of important and sensitive areas such as national defense facilities, military management zones, and national defense research and production units;

(5) 出口管制物项涉及的核心技术、设计方案、生产工艺等相关数据，密码、生物电子信息、人工智能等领域对国家安全、经济竞争力有直接影响的科学技术成果数据；

Data related to core technologies, design programs, production processes, etc. involved in export-controlled items, and data on scientific and technological achievements in the fields of cryptography, bio-electronic information, artificial intelligence, etc., which have a direct impact on national security and economic competitiveness;

(6) 国家法律、行政法规、部门规章明确规定需要保护或者限制处理的国家经济运行数据、重要行业和领域业务数据、统计数据等；

National economic operation data, business data of important industries and fields, and statistical data, the processing of which needs to be protected or restricted as stipulated by national laws, administrative regulations, departmental rules, and regulations;

(7) 其他一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。

Other data that may jeopardize national security, economic operation, social stability, public health and safety, etc. once tampered with, damaged, leaked,

or illegally accessed or illegally utilized.

Q4: 如何识别“敏感个人信息”？

How to identify "sensitive personal information"?

A4: 敏感个人信息，是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。[4]

Sensitive personal information refers to the personal information that is likely to result in damage to the personal dignity of any natural person or damage to the safety of his or her physical body or property once disclosed or illegally used, including information such as biometric identification, religious belief, specific identity, medical health, financial account, and whereabouts and tracks, etc., as well as the personal information of minors under the age of 14.

可参考国家标准 GB/T 35273-2020《信息安全技术个人信息安全规范》中关于个人敏感信息的定义及相关举例。

Reference can be made to the definition of personal sensitive information and related examples in the national standard GB/T 35273-2020 "Information Security Technology—Personal Information Security Specification".

Q5: 如何界定“关键信息基础设施运营者”？

Who is a "critical information infrastructure operator"?

A5: 根据《关键信息基础设施安全保护条例》，关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信

[4] 《中华人民共和国个人信息保护法》（全国人民代表大会常务委员会，主席令第九十一号，2021.08.20 发布，2021.11.01 实施）第 28 条规定。
Article 28, Personal Information Protection Law of the People's Republic of China (Order No. 91 of the President of the People's Republic of China, Standing Committee of the National People's Congress, issued on 20 August 2021, effective from 1 November 2021)

息系统等。

According to the Regulation on Protecting the Security of Critical Information Infrastructure, critical information infrastructure ("**CII**") refers to the network facilities and information systems in important industries and fields such as public telecommunications, information services, energy, transportation, water conservancy, finance, public services, e-government and science, technology and industry for national defense, as well as other important network facilities and information systems which, in case of destruction, loss of function or leak of data, may result in serious damage to national security, the national economy and the people's livelihood and public interests.

根据该规定，关键信息基础设施运营者的认定规则由各重要行业和领域的主管部门、监管部门（"保护工作部门"）制定，保护工作部门应及时将认定结果通知关键信息基础设施运营者，并通报国务院公安部门。

According to the provision, the rules for the determination of CII operators shall be formulated by the competent authorities and supervisory departments of each important industry and field ("Protection Working Departments"), and the Protection Working Departments shall promptly notify the CII operators of the results of the determination and notify the public security department of the State Council.

因此，建议数据处理者及时关注保护工作部门的通知，来判断自身是否构成关键信息基础设施运营者。

Therefore, it is recommended that data processors pay attention to the notification of the Protection Working Departments from time to time to determine whether they constitute a CII operator.

Q6: 如何界定 100 万、10 万、1 万的数量规模？

How to define the quantitative scale of 1 million, 100 thousand, and 10 thousand?

A6: 前文 Q1 中 100 万、10 万和 1 万的数量计算单位为"人"，而非"人次"或"条数"，数量规模统计中若存在重复计算的，应标明是否去重及去重依据。

The unit of calculation for the quantities of 1,000,000, 100,000, and 10,000 in Q1 above is "person", not "person-time(s)" or "number of pieces". If there is any double-counting in the statistics of the quantity scale, it should be indicated whether it is deduplicated or not and the basis for deduplication.

同样的，针对申报材料中的拟出境数据情况，基于《数据出境安全评估办法》第十四条要求，“通过数据出境安全评估的结果有效期为 2 年，自评估结果出具之日起计算”，对应数据规模应填写未来两年出境数据的规模和涉及自然人数量，自然人数量应按人数计算，并标明是否去重及去重依据（如涉及）。

Similarly, with regard to the intended outbound data in the declaration materials, based on the requirements under Article 14 of Measures for the Security Assessment of Outbound Data Transfers, which states that "the result of security assessment for an outbound data transfer is valid for two years, commencing from the date on which the result of the assessment is issued", the scale of the data shall correspondingly be filled in with the scale of the data to be exported in the next two years and the number of natural persons involved. The number of natural persons should be calculated on the basis of the number of persons, and whether or not the data have been deduplicated and the basis for deduplication (if relevant) should be indicated.

Q7: 同一数据处理者存在多个出境场景需要申报时应如何处理？

What should be done when there are multiple outbound scenarios to be declared by the same data processor?

A7: 数据处理者应在申报材料中说明是否符合数据出境安全评估申报条件，并需明确阐述具体符合《数据出境安全评估办法》第四条中的哪种情形（详见上文 Q1）。针对适用累计数量条件（即自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息）的，需要在申报材料中具体说明累计向境外提供的个人信息/敏感个人信息与本次申报出境数据的关系，以及对照《个人信息保护法》和《数据出境安全评估办法》开展的整改情况（如涉及）。

The data processor shall state in the declaration materials whether it meets the

declaration conditions for security assessment for outbound data transfers, and is required to clearly state which situation in Article 4 of the Measures for the Security Assessment of Outbound Data Transfers is specifically met (for details, please refer to Q1 of the above). If the cumulative quantity condition applies (i.e., the cumulative provision of personal information of 100 thousand persons or sensitive personal information of 10 thousand persons abroad since January 1 of the previous year), it is necessary to specify in the declaration materials the relationship between the cumulative provision of personal information/sensitive personal information to abroad and the specific data to be sent abroad as declared in the declaration being made this particular time, as well as the status of the corrective actions carried out in accordance with the Personal Information Protection Law of the People's Republic of China and the Measures for Security Assessment of Outbound Data Transfers (if relevant).

如果数据处理者存在多个出境场景需要申报评估的，根据《浙江省数据出境安全评估申报工作问答（三）》《海南省数据出境安全评估申报常见问答（二）》，**原则上应合并申报，并在申报材料中对出境场景分别予以说明**。

If a data processor has multiple outbound scenarios to be declared for assessment, according to the "Questions and Answers on the Declaration of Security Assessment for Outbound Data Transfers in Zhejiang Province (III)" and the "Frequently Asked Questions on the Declaration of Security Assessment for Outbound Data Transfers in Hainan Province (II)", **in principle the multiple outbound scenarios should be merged and declared together and be individually explained in the declaration materials.**

Q8: 什么情况应当重新进行数据出境安全评估？

When should a security assessment for outbound data transfers be re-conducted?

A8: 数据出境安全评估结果并非一次性永久有效，有两种情况需要重新评估。

The result of the security assessment for outbound data transfers is not valid permanently. There are two scenarios under which a reassessment would be required.

(1) 有效期届满：结果出具之日起满 2 年（通过数据出境安全评估的结果有效期为 2 年，自评估结果出具之日起计算）；

Expiration of its validity: 2 years from the date of issuance of the result (the validity of the results of the security assessment for outbound data transfers is 2 years from the date of issuance);

(2) 安全评估结果依据的重点评估事项发生变化影响出境数据安全的，具体情形如下：

One of the key variables in the previous security assessment has changed and in return affected the security of outbound data, specifically:

(a) 向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；

Changes in the purpose, manner, scope, and type of data provided abroad and in the use and manner of data processing by overseas recipients, affecting the security of outbound data, or the extension of the period for which personal information and important data are kept outside of the territory;

(b) 境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；

Changes in data security protection policies and regulations and network security environment in the country or region where the overseas recipient is located, as well as other force majeure circumstances, changes in the actual control of the data processor or overseas recipient, and changes in the legal documents between the data processor and the overseas recipient, which affect the security of outbound data;

(c) 出现影响出境数据安全的其他情形。

Other circumstances that affect the security of outbound data.

有效期届满，需要继续开展数据出境活动的，数据处理者应当在有效期届满 60 个工作日前重新申报评估。[5]

Upon the expiration of the validity period, if there is a need to continue the data outbound transfer activities, the data processor should conduct a re-assessment 60 working days before the expiry date.

◆ **实操演练 2**

Practical Exercise 2

Q：申报主体如何确定申报材料中需填写的“拟出境数据情况”？

Q: How should the declaring entity determine the "intended outbound data" to be filled in the declaration materials?

A：因上文所述的 2 年有效期规定，数据处理者申报的出境数据应为未来两年的拟出境数据，包括数据规模和涉及自然人数量，自然人数量应按人数计算，并标注是否去重。

A: Due to the provision of the validity period of two years mentioned above, the outbound data declared by the data processor should be the intended outbound data for the next two years, including the scale of data and the number of natural persons involved, the number of natural persons should be calculated based on the number of persons, and it should be indicated whether it is deduplicated or not.

Q9: 企业是否必须事先开展自评估工作？若需要，需要提前多久开展？自评估工作应当评估哪些方面？

Is it necessary for companies to carry out the self-assessment exercise in advance? If so, how far in advance? What should be assessed in the self-assessment?

A9: 是的，符合条件的企业应当在申报数据出境安全评估前进行风险自评估，

[5] 《数据出境安全评估办法》（国家互联网信息办公室，国家互联网信息办公室令第 11 号，2022.07.07 发布，2022.09.01 实施）第 14 条规定。
Article 14, Measures for the Security Assessment of Outbound Data Transfers (Order No. 11 of the Cyberspace Administration of China, issued on 7 July 2022, effective from 1 September 2022)

并在申报阶段提交风险自评估报告。

Yes, eligible companies should conduct a self-risk-assessment before declaring a security assessment of data transfers and submit a self-risk-assessment report at the declaration stage.

根据《数据出境安全评估申报指南（第一版）》附件 3《数据出境安全评估申报书（模板）》中的承诺书，申报主体应当承诺“自评估工作为申报之日前 3 个月内完成，且至申报之日未发生重大变化”。因此，**自评估报告落款时间应为申报之日前 3 个月内**，且申报前若发生重大变化，应当重新评估。

According to the letter of commitment contained within the “Declaration Statement for Security Assessment of Outbound Data Transfers (TEMPLATE)" in Annex 3 of the "Guidelines for Application for Security Assessment of Outbound Data Transfers (First Edition)", the declarer shall undertake that "the self-risk-assessment shall be completed within three months prior to the date of the declaration, and that no significant changes have occurred prior to the date of the declaration". Therefore, **the self-risk-assessment report should be dated within three months prior to the date of declaration**, and reassessment should be conducted if significant changes occur.

自评估重点应当评估以下六个方面：

The self-assessment should focus on assessing the following six areas:

(1) **[合法性基础、正当性、必要性]** 数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；

[Basis of legality, legitimacy, necessity] The legality, legitimacy, necessity of the purpose, scope, manner, etc., of the outbound data transfers and data processing by overseas recipients;

(2) **[出境数据对国家安全、公共利益、个人或组织可能带来的风险]** 出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；

[Risks that outbound data may pose to national security, public interests, individuals, or organizations] The scale, scope, type, and sensitivity of

outbound data, and the risks that outbound data may pose to national security, public interests, and the legitimate rights and interests of individuals or organizations;

(3) **[境外接收方的安全保障能力]** 境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

[Security guarantee capability of the overseas recipient] The obligations the overseas recipient has committed to undertake, and whether the management and technical measures and capabilities to fulfill the responsibilities and obligations can guarantee the security of the outbound data;

(4) **[数据传输（过程中或传输后）风险及安全保障（包括个人信息权益维护）]** 数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

[Risks and security guarantee (including protection of personal information rights and interests) of data transmission (during or after transmission)] Risks of data being tampered with, damaged, leaked, lost, transferred, illegally obtained, illegally utilized, etc., during or after data outbound transfer, and whether the channels for the protection of personal information rights and interests are accessible;

(5) **[法律文件中约定的数据安全保护责任义务]** 与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务。

[Responsibilities and obligations for data security protection as agreed in legal documents] Whether or not the data security protection responsibilities and obligations are sufficiently allocated in contracts relating to outbound data transfers or other legally binding documents, etc. (hereinafter collectively referred to as legal documents) with the overseas recipient.

(6) **[其他]** 其他可能影响数据出境安全的事项。[6]

[6] 《数据出境安全评估办法》（国家互联网信息办公室，国家互联网信息办公室令第 11 号，2022.07.07 发布，2022.09.01 实施）第 5 条规定。
Article 14, Measures for the Security Assessment of Outbound Data Transfers (Order No. 11 of the

[Other] Other matters that may affect the security of outbound data transfers.

◆ 实操演练 3

Practical Exercise 3

C 公司因符合“处理 100 万人以上个人信息的数据处理者向境外提供个人信息”而申报数据出境安全评估，其内部已根据《个人信息保护法》的规定，进行了个人信息保护影响评估（PIA）。

Company C has declared a security assessment for outbound data transfers due to meeting the criteria of "data processors who processed personal information of over one million persons providing personal information abroad". They have conducted internally a personal information protection impact assessment report (PIA) in accordance with the provisions of the Personal Information Protection Law.

Q：该 PIA 是否可以作为自评估报告？

Q: Can the PIA serve as a self-assessment report?

A：不可以，二者评估维度基本相同，但 PIA 只针对标准合同，该 C 公司申报数据出境安全评估的自评估报告应该参照《数据出境安全评估申报指南（第一版）》要求制定。

A: No, it cannot. Although the assessment dimensions are fundamentally similar, the PIA is specifically for standard contracts, the self-assessment report for Company C's security assessment for outbound data transfers should be prepared in accordance with the requirements outlined in the "Guidelines for Application for Security Assessment of Outbound Data Transfers (First Edition)”.

Q10: 数据出境安全评估申报流程需要花多长时间？

How long does the security assessment filing process of outbound data transfers take?

A10: 考虑到数据出境安全评估申报前期准备工作的复杂性，企业应预留充足的内部时间用于组织申报相关材料和提交申报（含自评估时间）。

Cyberspace Administration of China, issued on 7 July 2022, effective from 1 September 2022)

Considering the complexity of the preparatory work for the declaration of security assessment for outbound data transfers, companies should reserve sufficient time for organizing internally the relevant declaration materials and the submission of the declaration (inclusive of time for self-assessment).

正式提交申报材料后，法规规定的申报流程总共约为57+N个工作日（N指补充材料及其审核的时间），若涉及对评估结果有异议申请复评的，时长将相应延长 15+N 个工作日（收到评估结果 15 个工作日内申请复评，N 为复评时间）。建议有数据出境安全申报需求的企业应提前规划数据出境安全评估申报工作，为后续网信办的审批流程留足时间。

After formally submitting the declaration materials, the declaration process stipulated in the regulations will take a total of about 57+N working days (N stands for the time for supplemental materials and review of the same). In the event that there is disagreement regarding the assessment result and an application for reassessment is made, the length of time will be extended by 15+N working days accordingly (the application for reassessment should be made within 15 working days upon receipt of the assessment result, and N stands for the time required for a reassessment). It is recommended that companies with the need for a security declaration of outbound data transfers should plan in advance, so as to leave enough time for the subsequent approval process of the cyberspace administration office.

(二) 个人信息出境标准合同备案 15 问

(II) 15 Questions on the Filing of the SC for Outbound Transfer of Personal Information ("SC Filing")

Q11: 签订标准合同进行数据出境活动的适用范围？

What is the scope of application of a SC?

A11: 通常而言，通过订立标准合同的方式向境外提供个人信息的企业，应当**同时**符合下列情形：

Generally, a company that provides personal information abroad by entering into a SC shall meet the following circumstances **at any one given time**:

(1) 非关键信息基础设施运营者；

it is not a CII operator;

(2) 处理个人信息不满 100 万人的；

it processes the personal information of less than 1 million persons;

(3) 自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的；

it has cumulatively transferred abroad the personal information of less than 100 thousand persons since January 1 of the previous year; and

(4) 自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。

it has cumulatively transferred abroad the sensitive personal information of less than 10 thousand persons since January 1 of the previous year.

法律、行政法规或者国家网信部门另有规定的，从其规定。

Where there are other relevant provisions in any laws, administrative regulations, or rules of the Cyberspace Administration of China, such provisions shall apply.

企业不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。[7]

[7] 《个人信息出境标准合同办法》（国家互联网信息办公室国家互联网信息办公室令第 13 号

Companies shall not employ methods such as quantity splitting. They should abide by the law to provide personal data abroad via a SC in situations where one should have passed the security assessment for outbound data transfers as to personal information.

特别地，根据《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》的规定，注册于或位于粤港澳大湾区内地部分（即广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市，下称“粤港澳大湾区内地部分”）或香港特别行政区的个人信息处理者及接收方可以通过订立标准合同的方式进行粤港澳大湾区内内地和香港之间的个人信息跨境流动，构成重要数据的个人信息除外。

In particular, according to the "Implementation Guidelines on the Standard Contract for Cross-boundary Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)", PIP and the recipient registered or located in the Mainland part of Guangdong-Hong Kong-Macao Greater Bay Area (i.e., Guangzhou City, Shenzhen City, Zhuhai City, Foshan City, Huizhou City, Dongguan City, Zhongshan City, Jiangmen City, and Zhaoqing City in Guangdong Province, "**the Mainland part of the Guangdong-Hong Kong-Macao Greater Bay Area**") and the Hong Kong Special Administrative Region (HKSAR) may, by way of entering into a standard contract, carry out cross-border flow of personal information (excluding important data) between the Mainland and Hong Kong within the Guangdong-Hong Kong-Macao Greater Bay Area.

Q12: 标准合同签署的主体有哪些？

Who are parties to a SC?

A12: 涉及两类主体：个人信息处理者与境外接收方[8]。

2023.02.22 发布 2023.06.01 实施）第 4 条规定。
Article 4, Measures for the Standard Contract for Outbound Transfer of Personal Information (Order No. 11 of the Cyberspace Administration of China, issued on 2 February 2023, effective from 1 June 2023)

[8] 《个人信息出境标准合同办法》（国家互联网信息办公室，国家互联网信息办公室令第 13 号 2023.02.22 发布 2023.06.01 实施）第 2 条规定。
Article 2, Measures for the Standard Contract for Outbound Transfer of Personal Information (Order No. 11 of the Cyberspace Administration of China, issued on 2 February 2023, effective from 1 June 2023)

Mainly two types of entities: PIP and overseas recipients of such data.

◆ 实操演练 4

Practical Exercise 4

境外 D 公司直接通过网站为境内自然人用户提供服务，自上年 1 月 1 日起累计收集境内自然人用户个人信息不满 10 万人。

Overseas company D directly provides services to domestic natural person users through its website and has collected personal information from fewer than 100,000 natural person users since 1 January of the previous year.

Q：该境外 D 公司需要办理个人信息出境标准合同备案吗？

Q: Does the overseas company D need to conduct filing of the Standard Contract for Outbound Transfer of Personal Information?

A：不需要。个人信息处理者通过与境外接收方订立个人信息出境标准合同的方式向境外提供个人信息的，才适用《个人信息出境标准合同办法》进行备案。该情形下，仅有个人信息处理者境外 D 公司单一主体，不存在订立标准合同的场景条件，无需办理标准合同备案。但该场景构成“以向境内自然人提供产品或者服务为目的”，仍应当遵守《个人信息保护法》的各项要求。

A: No, it is not required. The filing under Measures for the Standard Contract for Outbound Transfer of Personal Information is applicable only when the personal information processor provides personal information abroad through the entering into a SC with the overseas recipients. In that case, as the overseas company D is the only entity as the PIP, and no condition of scenario for entering into the SC exists, there is no need to conduct filing of the SC. However, this scenario still falls under the category of "where the purpose is to provide domestic natural persons with products or services" and should comply with the various requirements of the Personal Information Protection Law.

Q13: 规定提及“自主缔约”，这是否意味着企业可以跳过备案环节？

The provision refers to "independent contracting", does this mean that companies can skip the filing process?

A13: 不可以，虽然不同于数据安全评估的事前监管，标准合同备案属于**事后监管**，但企业应当依法在标准合同生效后 10 个工作日内进行备案。

No. Although, unlike the prior supervision of security assessment for data, the filing of a SC is by nature *ex post* supervision, the company should still file the SC within 10 working days after its entry into force in accordance with the law.

为保障个人信息跨境安全、自由流动，通过订立标准合同的方式开展个人信息出境活动，《个人信息出境标准合同办法》确立了核心原则——“自主缔约与备案管理相结合、保护权益与防范风险相结合”。[9]该“自主缔约”是基于合同自愿原则，双方自行缔约（双方订立的其他与个人信息出境活动相关的合同，不得与标准合同的内容相冲突），但一旦采取该标准合同方式进行数据出境，即应当依法向所在地省级网信部门进行备案。

In order to safeguard the safe and free flow of personal information across borders, and to carry out outbound activities of personal information through a SC, the Measures for the Standard Contract for Outbound Transfer of Personal Information establishes the core principles - "combining independent contracting with record management, and combining the protection of rights and interests with the prevention of risks". The "autonomous contracting" is based on the principle of contractual voluntariness, and both parties contract on their own (other contracts related to outbound transfer activities of personal information concluded by both parties shall not conflict with the content of the SC), but once the SC is adopted for outbound data transfers, it shall be filed with the local provincial cyberspace administration department in accordance with the law.

特别地，如涉及个人信息在粤港澳大湾区内地部分与香港特别行政区之间跨境流动的，个人信息处理者及接收方均需在标准合同生效之日起 10 个工作日内按照属地向广东省互联网信息办公室或者香港特别行政区政府政府资讯科技总监办公室进行标准合同备案。

In Particular, if it involves the cross-border flow of personal information between

[9] 《个人信息出境标准合同办法》（国家互联网信息办公室，国家互联网信息办公室令第 13 号 2023.02.22 发布 2023.06.01 实施）第 3 条规定。
Article 3, Measures for the Standard Contract for Outbound Transfer of Personal Information (Order No. 13 of the Cyberspace Administration of China, issued on 2 February 2023, effective from 1 June 2023)

the Mainland part of the Guangdong-Hong Kong-Macao Greater Bay Area and the HKSAR, both the PIP and the recipient shall, according to the jurisdiction concerned, conduct the filing procedures of the Standard Contract with the Cyberspace Administration of Guangdong Province or the Office of Government Chief Information Officer of the HKSAR Government within 10 working days from the effective date of the Standard Contract.

Q14: 能否针对多个数据出境场景使用同一套标准合同？

Can the same set of SC be used for multiple outbound data transfers?

A14: 可以，可以针对多个数据出境场景使用同一套标准合同。

Yes, the same set of SC can be used for scenarios with multiple outbound data transfers.

如果数据出境活动涉及的数据出境方和境外接收方相同，且数据出境的目的相同，那么即便存在多个数据出境场景，亦可以使用一套标准合同，一次性办理备案。但如果数据出境方和境外接收方不同，则应当分别签订标准合同，分别办理标准合同备案。

If the outbound data transfer activities involve the same data exporter and overseas recipient, and the purposes of outbound data transfers are the same, then even if there are multiple outbound data transfers, one SC can be filed for the multiple outbound data transfers in one go. However, if the data exporter and overseas recipient are different, separate SCs should be signed and filed.

◆ 实操演练 5

Practical Exercise 5

云南 E 公司因业务经营与人事管理，需要向位于法国的总部 F 公司传输个人信息（场景包含通过 Workday 传输员工个人信息、通过 Salesforce 传输客户个人信息以及通过 CRM 系统传输消费者个人信息），云南 E 公司在境内五个省分别设有分支机构，员工、客户、消费者合计人数不足 5000 人。

Yunnan Company E needs to transfer personal information to its headquarter Company F in France (the scenario includes transferring employee personal information through Workday, customer personal information through Salesforce, and consumer personal information through the CRM system) due to its business operations and personnel management. Yunnan Company E has branch offices in five provinces within China, with a total of less than 5,000 employees, customers, and consumers.

Q：该 E 公司可以合并办理个人信息出境标准合同备案吗？

Q: Can Yunnan Company E consolidate the filing of SCs?

A：可以。云南 E 公司存在多个出境场景需要备案，境外接收方为单一主体，可以通过订立一套标准合同的方式合并备案（根据《云南省个人信息出境标准合同备案指引》，如果申请人存在多个出境事项（场景）需要备案，原则上合并备案，并在材料中分事项予以说明）。

A: Yes, they can. There is multiple outbound transfers from Yunnan Company E that require filing, with one single overseas recipient, where they can consolidate the filing by establishing a set of standard contracts (according to the "Filing Guidelines of Yunnan Province Standard Contract for Outbound Transfer of Personal Information", if the applicant has multiple outbound matters or scenarios which require filing, they should generally consolidate the filing and provide explanations for each item in the materials).

特别地，采取合并备案方式，一旦某一场景触发重新备案的条件的，则应当重新备案（详见下文 Q20），提醒个人信息处理者提前权衡利弊。

In particular, when adopting the consolidation of filing method, if a specific scenario triggers the conditions for re-filing, it should be refiled (see Q20 below). PIPs should be reminded to carefully consider the pros and cons in advance.

个人信息的出境场景因企业业务和性质不同而有较大差异，建议跨国公司结合自身业务及特点，仔细、全面梳理出境场景，避免遗漏。

The outbound scenarios of personal information vary significantly due to the business and nature of the company. It is recommended that the multi-national corporations carefully and comprehensively review their outbound scenarios based on their own business and characteristic as to avoid any mistakes.

Q15: 关联方是否可以合并备案？

Can related parties consolidate their filings?

A15: 标准合同的备案是向申报主体所在地的省级网信办进行备案，一般而言，对于不在同一省级行政区的关联方，应当分别与境外接收方签订标准合同并向各自所在地的省级网信办进行备案。对于存在不同的境外接收方，也建议分别签订标准合同并进行备案。

The SC Filings are to be made with the cyberspace administration at the provincial level where the declarer is located. Generally speaking, for related parties which are not in the same provincial administrative region, a separate SC should be signed between them and the overseas recipients and be filed with the cyberspace administration at the provincial level where the concerned related parties are located. For the existence of different overseas recipients, it is also recommended that separate SCs be signed and filed.

但针对同一集团公司项下多家独立法人企业的，根据公开信息检索，目前，已有北京市、湖南省、江西省、云南省、河北省、河南省、新疆生产建设

兵团等省级网信部门发布问答，明确“标准合同的备案主体须为法人实体，且备案主体应与境内合同签署方一致。**如多家独立法人企业同属一家集团公司，可由集团公司作为个人信息出境标准合同备案主体**。分公司不具备独立法人，不可代替总部或子公司备案。”若企业选择合并由集团公司备案的，建议提前关注集团公司所在地省级网信部门的指导意见，并事先咨询确认。

However, for various independent legal person corporations of the same parent group, according to public information retrievable to date, cyberspace administration at the provincial level, including Beijing, Hunan Province, Jiangxi Province, Yunnan Province, Hebei Province, Henan Province, Xinjiang Production and Construction Corps etc. have issued Q & A, clearly stating that "the entity filing a SC must be a legal person entity, and the same party should be the signatory to the SC within the territory. **For various independent legal person corporations belonging to the same parent group, the parent company can be the responsible entity for the entering and filing of a SC**. For branch corporations that are not independent legal persons, they may not replace the parent company or subsidiaries for filing." If corporations decide to consolidate and have the parent company file a SC, it is recommended to pay attention to the guidance opinion of the cyberspace administration at the provincial level where the parent company is located, along with consultation and confirmation.

特别地，采取合并备案方式，一旦某一主体触发重新备案的条件的，则应当重新备案（详见下文 Q20），提醒个人信息处理者提前权衡利弊。

In particular, by adopting a consolidated filing approach, once a subject entity triggers the condition for re-filing, it should re-file (see Q20 below for details), and PIPs are reminded to weigh the pros and cons in advance.

◆ 实操演练 6

Practical Exercise 6

总部在英国的化妆品零售业 G 集团，在北京设立了大中华区控股公司 H 公司，并由 H 公司于上海、广东、湖南等地设立了子公司，使用统一的集团管理系统，G 集团可以在英国访问北京、上海、广东、湖南的销售数据（含消费者个人信息）。

G Group, a cosmetics retail business company with its headquarters in the UK, established a Greater China holding company, Company H, in Beijing, and set up subsidiaries in places like Shanghai, Guangdong, and Hunan through Company H. G Group uses a unified group management system, where they can access the sales data (including personal information of consumers) of Beijing, Shanghai, Guangdong, and Hunan while situating in the UK.

Q：四家中国主体分别办理标准合同备案，还是选择合并办理？

Q: Should the four Chinese entities separately file the SCs, or should they choose to consolidate the filing?

A：根据现有数据流，应当分别申报，但因北京市网信办认可由集团公司作为备案主体（详见上文），可在事前与主管部门进行咨询确认的基础上，选择合并申报。

A: Based on the current data flow, they should file separately. However, since the Cyberspace Administration office in Beijing acknowledges that the group company can act as the filing entity (see above), they can choose to consolidate the filing after consultation and confirmation with the competent authorities in advance.

特别地，若在申报前，集团公司基于内部数据管理进行数据流调整，境内子公司数据先行汇总到北京控股公司 H 公司，由 H 公司统一提供给 G 集团，则可以直接由 H 公司进行标准合同备案。

In particular, if, before filing, the group company adjusts the data flow based on internal data management and aggregates data from local subsidiaries to Company H, the holding company in Beijing, which is then provided to G Group in a unified manner, filing of the SC can be done by Company H directly.

Q16: 可以修改标准合同条款吗？

Can the terms of a SC be modified?

A16: 不可以，标准合同的文本内容不得修改。个人信息处理者与境外接收方应当严格按照标准合同模板订立合同，不得修改或删除标准合同正文中的任一条款。在不与标准合同正文内容相冲突的前提下，双方如有其他约定可在标准合同的附录二中详述，附录构成标准合同的组成部分。

No. The terms of the SC shall not be modified. The PIP and the overseas recipient shall enter into a contract in strict accordance with the SC template and shall not modify or delete any of the clauses contained within. Provided the absence of conflict with the terms of the SC, other agreed terms between the parties may be detailed in Appendix II of the SC, forming an integral part of their contract.

Q17: 如果已签署 GDPR 下的标准合同, 是否还需签署中国的标准合同？

If a SC under the GDPR has been signed, do I need to sign a SC that conforms with the Chinese laws?

A17: 仍然需要。

Yes.

GDPR 标准合同适用于从欧盟国家向第三国出境个人信息，而中国标准合同适用于从中国向第三国出境个人信息，二者传输路径具有很大差异，GDPR 下的标准合同无法作为从中国向其他国家传输个人信息的合法依据。

The GDPR SC applies to the outbound provision of personal information from an EU country to a third country, while the Chinese SC applies to the outbound provision of personal information from China to a third country, and the transmission paths of the two are so different that the standard contract under the GDPR cannot be used as a legal basis for the transfer of personal information from China to other countries.

Q18: 个人信息处理者是否可以提交非中文版标准合同？

Can a PIP submit a non-Chinese version of a SC?

A18: 原则上，个人信息处理者应当提交中文版标准合同（中英双语标准合同亦可，但建议注明如有差异，以中文版为准）。

In principle, PIPs should submit a SC in Chinese (a bilingual version is also acceptable, but one is recommended to state clearly that in case of discrepancies, the Chinese version prevails).

若仅有非中文版本，须同步提交准确的中文译本，中文译本形式（如个人信息处理者盖章承诺译本内容与原版一致，或是要求第三方公证等形式）建议与所在地省级网信部门提前咨询确认。

If there is only a non-Chinese version, then an accurate Chinese translation must be submitted together, and one recommends that the form of the Chinese translation (e.g., the PIP seals to promise that the content of the translation is the same as the original version, or requesting a third-party notarization, etc.) be confirmed in advance by consulting the local cyberspace administration department at the provincial level.

Q19: 标准合同备案的有效期多久？

How long is a filing of SC valid for?

A19: 不同于数据出境安全评估存在两年有效期（详见上文Q8）的法定要求，标准合同并无有效期的强制规定，个人信息处理者可以与境外接收方基于个人信息出境的具体场景，在满足《个人信息保护法》规定的情形下（如最小必要原则），约定适当的有效期。

Unlike the statutory requirement of a two-year validity period for the security assessment for outbound data transfers (see Q8 above for details), there is no mandatory validity period for the SC, and the PIP may agree with the overseas recipient on an appropriate validity period based on the specific scenario of the outbound transfer of personal information, provided that it meets the provisions of the Personal Information Protection Law (e.g., the principle of minimum necessity).

Q20: 什么情况下需要重新备案？

Under what circumstances will it be necessary to re-file?

A20: 在标准合同有效期内出现下列情形之一的，个人信息处理者应当重新开展PIA，补充或者重新订立标准合同，并履行相应备案手续：

Where any of the following circumstances occur during the validity period of the SC, the PIP shall conduct the personal information protection impact assessment again, supplement or re-sign the SC, and conduct relevant record-filing formalities:

(1) 向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的；

the purpose, scope, category, sensitivity, method, and storage location of personal information transferred abroad, or the purpose and method of personal information processing by the overseas recipient has changed, or the retention period of personal information located abroad is extended;

(2) 境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的；

the personal information rights and interests will be affected by the changes in the policies and regulations on personal information protection in the country or region where the overseas recipient is located; or

(3) 可能影响个人信息权益的其他情形。[10]

other circumstances that may affect the personal information rights and interests.

个人信息处理者在标准合同有效期内补充订立标准合同的，应当向所在地省级网信办提交补充材料；重新订立标准合同的，应当重新备案。补充或

[10] 《个人信息出境标准合同办法》（国家互联网信息办公室，国家互联网信息办公室令第 13 号 2023.02.22 发布 2023.06.01 实施）第 8 条规定。
Article 8, Measures for the Standard Contract for Outbound Transfer of Personal Information (Order No. 11 of the Cyberspace Administration of China, issued on 2 February 2023, effective from 1 June 2023)

者重新备案的材料查验时间为 15 个工作日。

Where a supplemental agreement is entered into within the validity period of a pre-existing SC, the PIP shall submit supplementary materials to the concerned local provincial cyberspace administration office. Re-filing is necessary where a new SC has been entered into. The time frame for the review of the supplemental or re-filed materials is 15 working days.

个人信息处理者对所提交材料的真实性负责，提交虚假材料的，按照备案不通过处理，并依法追究相应法律责任。[11]

The PIP shall be responsible for the authenticity of the materials submitted. In case of false materials submitted, the filing shall be deemed as a failure and the PIP to bear any corresponding legal liabilities so arising.

◆ 实操演练 7

Practical Exercise 7

境内 J 公司委托境外 K 公司处理个人信息，依法订立了标准合同并办理备案。但有效期内，因业务所需，需要延长个人信息境外保存期限。

Domestic Company J entrusted overseas Company K to process the personal information and has legally entered into a SC and the filing has been completed. However, due to the business needs, they need to extend the overseas storage period for personal information within the validity period.

Q：境内 J 公司与境外 K 公司只能重新签订标准合同并重新进行备案吗？

Q: Can Domestic Company J and Overseas Company K only re-sign the standard contract and re-file it?

A：不是。“延长个人信息境外保存期限”属于法定应当重新开展 PIA 的情形，J 公司与 K 公司除了重新签订标准合同外，可以考虑通过在标准合同的附件二其他条款中完善或签订补充协议等方式补充，而非仅能重新订立标准合同。一定程度上，可以避免重新谈判的负担。

[11] 《个人信息出境标准合同备案指南（第一版）》（国家互联网信息办公室，2023.05.30 发布，2023.05.30 实施）“三、备案流程”规定。
3. Filing Process, Guidelines for Filing Standard Contract for Outbound Transfer of Personal Information (First Edition) (Cyberspace Administration of China, issued on 30 May 2023, effective from 30 May 2023)

A: Not necessarily. "Extending the overseas storage period for personal information" falls under the situation where a PIA should be conducted again. Apart from re-signing the SC, Company J and Company K may consider supplementing it by amending other clauses in Appendix 2 of the SC or signing a supplemental agreement, rather than entering into a new SC. To some extent, this can help avoid the burden of renegotiation.

Q21: 受托人是否可以签订标准合同？

Can a trustee enter into a SC?

A21: 根据《个人信息出境标准合同办法》的规定，标准合同应在个人信息处理者和境外数据接收方之间签署并实施。**出境方为个人信息处理者，境外接收方可能是个人信息处理者或者受托处理个人信息的受托人**。

According to the "Measures for the Standard Contract for Outbound Transfer of Personal Information", a SC shall be signed and implemented between the PIP and the overseas recipient of the data. **The data exporter is the PIP, and the overseas recipient could be a PIP or a trustee entrusted with the processing of personal information.**

但实践中因个人信息处理者与受托人界定不清，也存在受托人办理标准合同备案的情形。若是作为受托人受托处理个人信息而需向境外接收方传输的，建议提前咨询所在地省级网信部门意见。

However, in practice, due to the unclear definition of a PIP and a trustee, there are also cases where the trustee handles the SC Filing. If a trustee is entrusted with the processing of personal information and needs to transmit the same to overseas recipients, one is recommended to consult the local cyberspace administration department at the provincial level in advance.

◆ 实操演练 8

Practical Exercise 8

境内 L 公司向境外集团总部 M 公司传送境内员工个人信息，位于美国的关联公司 N 公司可以查看上述个人信息。

Company L, a company within the territory, transmits personal information of domestic employees to Company M, the headquarters of Group, located overseas. Affiliated Company N, located in the United States, is able to access the aforementioned personal information.

Q：境内 L 公司需要与 M 公司、N 公司分别订立标准合同并备案吗？

Does Company L within the territory need to separately enter into SC with Company M and Company N and file them?

A：不需要。根据国家网信办制定的《个人信息出境标准合同》附录一《个人信息出境说明》，上述情形，可以将 N 公司作为“境外接收方只向以下中华人民共和国境外第三方提供个人信息（如适用）”中的第三方进行披露，因此，境内 L 公司仅需与 M 公司订立标准合同，并在标准合同内披露 N 公司的访问事宜即可。

Not necessary. According to Appendix 1 ‘Explanation on the Cross-border Transfer of Personal Information’ of the SC formulated by the Cyberspace Administration of China, in the aforementioned situation, N company can be disclosed as a “Overseas Recipients that only provides personal information (if applicable) to the following third parties outside the territory of the People's Republic of China”. Therefore, Company L only needs to enter into a SC with Company M and disclose the access of Company N within the SC.

特别地，该情形下，M 公司仍应当注意满足标准合同中约定的相关义务（如 M 公司与 N 公司签署书面协议、确保 N 公司的个人信息处理活动达到我国相关法律法规规定的个人信息保护标准等）；同时，N 公司访问 L 公司传送给 M 公司的数据，可能构成 M 公司所在国的数据出境，应注意满足当地法律法规的要求。

In particular, in this situation, Company M should still pay attention to fulfilling the relevant obligations stipulated in the SC (such as signing a written agreement with Company N, ensuring that the processing of personal information by Company N meets the personal information protection standards as required by relevant laws and regulations in our country). At the same time, when Company N accesses the data transmitted by Company L to Company M, it may constitute outbound data transfers to the country where Company M is located, so attention should be paid to meeting the requirements of local laws and regulations of Company M.

Q22: 在标准合同备案路径下，PIA 是否有特殊之处？

Is PIA special under the SC Filing path?

A22: PIA 工作应当在备案之日前 3 个月内完成，且至备案之日未发生重大变化。

The PIA work should be completed within three months prior to the date of filing and with no significant changes between the date of the PIA work and the filing date.

个人信息处理者应当保存个人信息保护影响评估报告至少 3 年。

PIPs shall keep the personal information protection impact assessment report for at least three years.

通常情形下，标准合同备案时需要提交个人信息保护影响评估报告；但在粤港澳大湾区内地部分与香港特别行政区的个人信息跨境流动情形下，无需递交。

Generally, a personal information protection impact assessment report is required to be submitted for the filing of a standard contract; however, it is not required in the case of the cross-border flow of personal information between the Mainland part of the Guangdong-Hong Kong-Macao Greater Bay Area and the HKSAR.

Q23: 标准合同备案的结果是什么？

What is the outcome of a SC Filing?

A23: 备案结果分为通过、不通过。

The filing results are divided into Pass and Failure.

通过备案的，省级网信办向个人信息处理者发放备案编号；不通过备案的，个人信息处理者将收到备案未成功通知及原因，要求补充完善材料的，个人信息处理者应当补充完善材料并于 10 个工作日内再次提交。在获得“通过”结果前, 建议企业暂停相关个人信息的出境活动。

For PIPs who passed the filing, the provincial cyberspace administration office will issue them a filing number. For PIPs who fail to pass the filing, the PIP will

receive a notice on unsuccessful filing and the reasons therefor. For cases where the PIP is required to supplement and perfect the materials, the PIP shall do so and resubmit its filing again within ten working days. Before obtaining the "Pass" result, it is recommended that the company suspends any outbound activities of personal information.

Q24: 宽限期内的个人信息跨境传输是否合法？

Are outbound transfers of personal information during the grace period legal?

A24: 《个人信息出境标准合同办法》自 2023 年 6 月 1 日起施行，并规定“本办法施行前已经开展的个人信息出境活动，不符合本办法规定的，应当自本办法施行之日起 6 个月内完成整改”。

Measures for the Standard Contract for Outbound Transfer of Personal Information has come into force since 1 June 2023, and stipulates that "[f]or the outbound transfer of personal information that has already happened before the Measures takes effect, if it is found that any such transfer is not in compliance with the Measures, rectification shall be completed within 6 months upon the effective date of the Measures."

意味着，若个人信息处理者符合标准合同备案的适用条件，且在 2023 年 6 月 1 日前已经开展个人信息出境活动的，可以在 6 个月的宽限期内继续传输个人信息，但应当在 2023 年 11 月 30 日之前订立标准合同并进行备案。2023 年 11 月 30 日后，如果未能完成整改的，应暂停出境，直至完成。

In other words, if a PIP falls within the category of having to file for a SC but has already been carrying out outbound transfer activities of personal information before 1 June 2023, it may continue to transmit personal information during the 6-month grace period. However, it should enter into a SC and file it before 30 November 2023. After 30 November 2023, if it fails to complete the rectification, it should suspend all its outbound activities until after completion.

Q25: 若未能在宽限期内完成整改，数据出境是否非法？是否需承担责任？

In the event that modification is not completed within the grace period, would

the outbound data transfer be illegal? Is there any legal consequence for such a failure?

A25: 是非法的（本处指亦未选择个人信息保护认证路径的情形），且应当依法承担责任。

Yes, it is illegal (this refers to cases where the personal information protection certification path has not been selected either) and shall be held liable in accordance with the law.

(1) 行政责任：《个人信息出境标准合同办法》援引《个人信息保护法》对违规行为进行处罚规制，包括责令改正，给予警告，没收违法所得等，最高适用 5000 万元人民币或上一年度营业额 5%的罚款，并可责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照。此外，企业直接负责的主管人员和其他直接责任人员（如 DPO）可能被追究个人责任，包括被处以最高 100 万元人民币的罚款，并可禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。

Administrative Liability: Measures for the Standard Contract for Outbound Transfer of Personal Information quote the Personal Information Protection Law which imposes penalties for non-compliance, including ordering corrections, giving warnings, confiscating illegal income, etc., and applying fines of up to RMB 50 million or 5% of the turnover of the previous year, as well as ordering the suspension of the relevant business or the closure of the business, informing the relevant competent authorities for the revocation of the relevant business permits or the revocation of business licenses. In addition, directly responsible supervisors and other directly responsible persons of the company (such as DPO) may be held personally liable, including being fined up to RMB 1 million, and may be prohibited from serving as directors, supervisors, senior management and persons in charge of personal information protection of the relevant company for a certain period.

(2) 民事责任：个人信息主体也可因损害其合法权益而提起民事诉讼。

Civil liability: The owner of the personal information may also bring a civil action for damage to his or her legal rights and interests.

特别地，按照现有《个人信息出境标准合同》模板，**其将该合同义务履行的举证责任作为个人信息处理者的义务**（第二条 个人信息处理者的义务……（十）对本合同义务的履行承担举证责任），**意味着，对境内出境方提出了更高的要求，一旦出现争议情形，即便是应由境外接收方来履行的义务，在触发监管或者诉讼时，都有可能直接要求境内出境方进行举证。建议境内出境方加强对于境外接收方的日常监督与管理，并注意留痕相应证据材料，以免承担举证不利的后果**。

In particular, the existing SC template **places the burden of proof for the fulfillment of the obligations under the SC on the PIP** (Article 2 The Obligations of the PIP ..... (x) The Burden of proof for the fulfillment of the obligations of this contract). **This means that a higher requirement is placed on the data exporters in the event that a dispute arises. In case of disputes, even if the obligations should be fulfilled by the overseas recipient, the data exporters may be directly required to provide evidence when regulation or litigation is triggered. It is recommended that the data exporters should strengthen the daily supervision and management of the overseas recipient and pay attention to leaving trails of corresponding evidential materials, so as to avoid the consequences of a failure to provide evidence when the need so arises**.

(3) 刑事责任：根据我国法律规定，构成犯罪的（如侵犯公民个人信息罪等），依法追究刑事责任。

Criminal Liability: According to the laws of China, any act that constitutes a crime (such as the crime of violating citizens' personal information, etc.), will be accounted for in accordance with the laws.

◆ 实操演练 9

Practical Exercise 9

境内 O 公司自 2022 年开始，每月 10 日前均将汇总整理上一月度境内业务 APP 运营中收集的消费者个人信息，并传送境外集团总部。

From 2022, Company O within the territory has been summarizing and organizing the personal information of consumers collected from the operation of its domestic APP before the 10th of each month, and transmitting it to the overseas headquarters of the Group.

2023 年 7 月，因跨境业务合作，准备将消费者个人信息传送境外第三方合作公司 P 公司。

In July 2023, in preparation for cross-border business cooperation, Company O intends to transfer the personal information of consumers to a third-party cooperating company, Company P, located overseas.

Q：2023 年 6 月起，境内 O 公司还能向集团总部进行传输吗？境内 O 公司可以向境外 P 公司传输吗？

Q: Starting from June 2023, can Company O within the territory continue to transmit data to the Group headquarters? Can Company O within the territory transmit data to Company P overseas?

A：须区分业务场景：

A: It is necessary to distinguish between different business scenarios:

针对面向集团总部的数据传输，若符合标准合同路径要求的（详见 Q11），境内 O 公司仍可以继续传送，但应当在 2023 年 11 月 30 日前与集团总部公司订立标准合同并进行备案。

Regarding the transmission of data to the Group headquarters, if it meets the requirements of the standard contract path (see Q11 for details), Company O within the territory can still continue to transmit data. However, it should enter into a SC with the Group headquarters company and complete the filing before 30 November 2023.

针对面向 P 公司的数据传输，其非在 2023 年 6 月 1 日前已经开展个人信息出境活动的，不符合上述宽限期适用条件，应当先行与 P 公司订立标准合同，并在标准合同生效之日起 10 个工作日内，通过送达书面材料并附带材料电子版的方式，向所在地省级网信办备案。否则，将构成非法行为，存在承担上述责任的风险。

Regarding the transmission of data to Company P, since the outbound transfer activities of personal information has not been engaged before 1 June 2023, the above-mentioned grace period conditions have not been met. Therefore, they should first enter into a SC with Company P and, within 10 working days from the effective date of the SC, submit written materials and electronic copies to the provincial-level Cyberspace Administration office for record filing. Otherwise, it will constitute an illegal act and carry the risk of assuming the aforementioned responsibilities.

(三) 个人信息跨境处理活动安全认证 5 问

(III) 5 Questions on Security Certification for Cross-border Processing Activities of Personal Information ("PIPC")

Q26: 何时可以选择个人信息跨境处理活动安全认证路径？

When can I choose the PIPC?

A26: 对于不适用数据出境安全评估，其业务范围涉及个人信息处理活动的企业，可自行选择采取标准合同备案或者个人信息跨境处理活动安全认证。

For companies whose business scope involves personal information processing activities but is not suitable for a security assessment for outbound data transfers, they may choose to adopt a SC Filing or PIPC instead.

如果企业符合以下两类主体标准，其更适合走安全认证路径：

If a company meets the criteria for the following two categories of subjects, it is more appropriate for it to follow the PIPC path:

(1) 跨国公司或同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动；

CPAPI between subsidiaries or affiliates of multinational corporations or the same economic or business entity;

(2) 《个人信息保护法》第 3 条第 2 款规定的境外个人信息处理者处理中国境内自然人个人信息的活动（在境外处理中国境内自然人个人信息的活动，有下列情形之一的，也适用本法：（一）以向境内自然人提供产品或者服务为目的；（二）分析、评估境内自然人的行为；（三）法律、行政法规规定的其他情形）。

Activities of overseas PIPs dealing with personal information of natural persons in China, as stipulated in Article 3, paragraph 2 of the Personal Information Protection Law (this Law shall also apply to the processing of the personal information of natural persons within the territory of the People's Republic of China outside the territory of the People's Republic of China

under any of the following circumstances: (i) where the purpose is to provide domestic natural persons with products or services; (ii) where the acts of domestic natural persons are analyzed and evaluated; and (iii) other circumstances as prescribed by laws and administrative regulations).

Q27: 是否可以选择安全认证来代替标准合同备案？

Is PIPC an alternative option to SC Filing?

A27: 可以，针对安全认证与标准合同备案路径均可适用的情形，**结合通过后的时效**（安全认证有效期 3 年[12]（详见下文 Q30），标准合同无强制有效期（详见上文 Q19））**以及便利程度**（安全认证除了需要标准合同备案路径下需要的合同以及 PIA 外，还需要委托第三方认证机构实施认证），现阶段仍更建议采取标准合同备案方式。

Yes, for situations whereby both the PIPC and SC Filing path are applicable, **considering the time limit after the passing** (PIPC is valid for three years (see Q30 below for details), the SC does not have a mandatory expiration date (see Q19 above for details)) **and the degree of convenience** (for PIPC, in addition to the contract and PIA required under the SC path, the commissioning of a third-party certification agency to do the certification is also required), the SC Filing route is preferable at this stage.

[12] 《个人信息保护认证实施规则》（国家市场监督管理总局，国家互联网信息办公室，国家市场监督管理总局，国家互联网信息办公室公告，2022 年第 47 号，2022.11.04 发布，2022.11.04 实施）之“5.1.1 认证证书的保持”。
5.1.1 Holding of Certification Certificate, Implementation Rules on Personal Information Protection Certification (State Administration of Market Regulation (SAMR), Cyberspace Administration of China(CAC), Announcement No.47 of 2022 of SAMR and CAC, issued on 4 November 2022, effective from 4 November 2022

◆ 实操演练 10

Practical Exercise 10

境外 Q 公司面向境内自然人，运营独立网站以销售其境外商品。

Overseas Company Q operates an independent website targeting domestic natural persons to sell its overseas goods.

Q：境外 Q 公司也可以用安全认证来代替标准合同备案吗？

Q: Can overseas Company Q use PIPC as a substitute for SC Filing?

A：不可以，该场景不适用标准合同备案路径（详见上文 Q12），境外 Q 公司应当通过安全认证路径出境。

No, this scenario does not fall within the scope of the SC Filing process (refer to Q12 above for more details). Overseas Company Q should comply with the law and obtain PIPC for outbound data transfers.

Q28: 安全认证路径下，是否需要指定个人信息保护负责人并设立个人信息保护机构？

Is it necessary to designate a person to be in charge of personal information protection and establish a personal information protection organization under the PIPC path?

A28: 需要，**个人信息处理者**和**境外接收方**均需要指定个人信息保护负责人，并设立个人信息保护机构。

Yes. Both **the PIP** and **the overseas recipient** are required to designate a person in charge of personal information protection and establish a personal information protection organization.

其中，个人信息保护负责人应具备个人信息保护专业知识和相关管理工作

经历，由该组织的决策层成员承担。[13]

In particular, the person in charge of personal information protection shall have expertise in personal information protection and relevant management experience and shall be a member of the decision-making level of the organization.

Q29: 安全认证具体怎么开展？

How is PIPC conducted?

A29: 企业开展安全认证的具体流程分为下述五个步骤：

The specific process for companies to carry out PIPC is divided into the five steps described below:

(1) **认证委托**：认证委托人应当按认证机构要求提交认证委托资料（包括但不限于认证委托人基本材料、认证委托书、相关证明文档等），认证机构在对认证委托资料审查后及时反馈是否受理。

Certification commission: The person commissioning certification shall submit materials for the certification commission in accordance with the requirements of the certification agency (including, but not limited to, the basic information of the person commissioning the certification, power of attorney for certification, relevant documents of proof, etc.), the certification agency will provide timely feedback on whether to accept the commission after reviewing the certification commissioning materials.

认证机构受理的，应当确定认证方案，包括个人信息类型和数量、涉及的个人信息处理活动范围、技术验证机构信息等，并通知认证委托人。

If the certification agency accepts the commission, it shall determine the

[13] 《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》（全国信息安全标准化技术委员会，信安秘字〔2022〕216 号，2022.12.16 发布 2022.12.16 实施）之“第 5.2 组织管理”。
5.2 Organization Management, Guidelines for Cybersecurity Standard Practice - Security Certification Specification for Cross-border Processing Activities of Personal Information V2.0 (National Information Security Standardization Technical Committee, No. 216 of 2022, issued on 16 December 2022, effective from 16 December 2022)

certification scheme, including the type and amount of personal information, the scope of personal information processing activities involved, and the information of the technical verification agency, and notify the person commissioning certification er.

(2) **技术验证**：技术验证机构应当按照认证方案实施技术验证，并向认证机构和认证委托人出具技术验证报告。

Technical verification: The technical verification agency shall implement technical verification in accordance with the certification scheme, and issue a technical verification report to the certification agency and person commissioning the certification.

(3) **现场审核**：认证机构实施现场审核，并向认证委托人出具现场审核报告。

On-site audit: the certification agency will implement an on-site audit, and issue an on-site audit report to the person commissioning the certification.

(4) **认证结果评价和批准**：认证机构根据认证委托资料、技术验证报告、现场审核报告和其他相关资料信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证委托人限期整改，整改后仍不符合的，以书面形式通知认证委托人终止认证。

Evaluation and approval of certification results: the certification agency will make a decision for certification based on the comprehensive evaluation made according to the materials for the certification commission, technical verification reports, on-site audit reports, and other relevant information. For cases that meet the certification requirements, a certificate of certification will be issued. For the ones that do not yet meet the certification requirements, the person commissioning the certification may be required to make rectifications before the deadline. If the certification agency finds that after rectification, the application is still not sufficient for certification purposes, then the agency will notify the person commissioning the certification in writing of the termination of the commission for certification.

如发现认证委托人、个人信息处理者存在欺骗、隐瞒信息、故意违反认证要求等严重影响认证实施的行为时，认证不予通过。

If it is found that the person commissioning the certification or PIP has committed acts that seriously affect the implementation of certification such as deception, concealment of information, or intentional violation of certification requirements, the certification will not be allowed.

(5) **获证后监督**：认证机构应当在认证有效期内，对获得认证的个人信息处理者进行持续监督（认证机构应当采取适当的方式实施获证后监督，确保获得认证的个人信息处理者持续符合认证要求），并合理确定监督频次。认证机构对获证后监督结论和其他相关资料信息进行综合评价，评价通过的，可继续保持认证证书；不通过的，认证机构应当根据相应情形作出暂停直至撤销认证证书的处理。

Post-certification supervision: The certification agency shall, within the validity period of the certification, carry out continuous supervision of the certified PIPs (the certification agency shall take appropriate measures to implement the post-certification supervision to ensure that the certified PIPs continue to comply with the certification requirements), and reasonably determine the frequency of supervision. The certification agency shall conduct a comprehensive evaluation of the outcomes of the post-certification supervision and other relevant information, and if the evaluation is passed, the concerned entity can keep the certification; if the evaluation is not passed, the certification agency shall suspend or revoke the certification accordingly.

Q30: 安全认证的有效期？

What is the validity period of the PIPC?

A30: 安全认证的认证证书有效期为 3 年。若证书到期需延续使用的，企业应在有效期届满前 6 个月内向认证机构提出认证申请。认证机构采用获证后监督的方式，对符合认证要求的颁发新证书。[14]

[14] 《个人信息保护认证实施规则》（国家市场监督管理总局，国家互联网信息办公室，国家市场

The PIPC is valid for three years. If after its expiration, one intends to continue activities that require one to have a valid certificate, then the company should make an application for certification at least 6 months before the certification expiration date. The certification agency will adopt the same compliance standard for post-certification supervision in evaluating whether a given applicant meets the requirement for the issuance of a new certification.

[以下无正文]

监督管理总局，国家互联网信息办公室公告，2022 年第 47 号，2022.11.04 发布，2022.11.04 实施）之“5.1.1 认证证书的保持”。

5.1.1 Holding of Certification Certificate, Implementation Rules on Personal Information Protection Certification (State Administration of Market Regulation (SAMR), Cyberspace Administration of China(CAC), Announcement No.47 of 2022 of SAMR and CAC, issued on 4 November 2022, effective from 4 November 2022

附件一：问题/案例索引

Annex I: Index of Q&As and Practical Exercises

附件二：主要法律法规一览表[15]

Annex II: List of Major Laws and Regulations

序号 No.	文件名称 Name of Document	发文机关 Issuing Body	发文时间 Issuing Date	生效时间 Effective Date	效力层级 Level of Strength
1	《中华人民共和国网络安全法》 "PRC Cybersecurity Law"	全国人民代表大会常务委员会 Standing Committee of the National People's Congress ("**SCNPC**")	2016.11.07	2017.06.01	法律 Law
2	《中华人民共和国数据安全法》 "PRC Data Security Law"	全国人民代表大会常务委员会 SCNPC	2021.06.10	2021.09.01	法律 Law
3	《中华人民共和国个人信息保护法》 "PRC Personal Information Protection Law"	全国人民代表大会常务委员会 SCNPC	2021.08.20	2021.11.01	法律 Law
4	《信息安全技术 个人信息安全规范（GB/T 35273—2020）》 "Information Security Technology - Personal Information Security Specification (GB/T 35273-2020)"	全国信息安全标准化技术委员会 National Information Security Standardization Technical Committee	2020.03.06	2020.10.01	推荐性国标 Recommended National Standard

[15] 暂未纳入各地网信部门发布的问答或者指引，请以官方发布为准。
Not yet included in the questions and answers or guidelines published by local cyberspace administration departments. Please refer to official publications for accurate information.

序号 No.	文件名称 Name of Document	发文机关 Issuing Body	发文时间 Issuing Date	生效时间 Effective Date	效力层级 Level of Strength
5	《数据出境安全评估办法》 "Measures for Security Assessment of Outbound Data Transfers"	国家互联网信息办公室 Cyberspace Administration of China	2022.07.07	2022.09.01	部门规章 Departmental Regulations
6	《数据出境安全评估申报指南（第一版）》 "Guidelines for Application for Security Assessment of Outbound Data Transfers (First Edition)"	国家互联网信息办公室 Cyberspace Administration of China	2022.08.31	2022.08.31	规范性文件 Normative Document
7	《个人信息出境标准合同办法》 "Method of Standard Contract for Outbound Transfer of Personal Information"	国家互联网信息办公室 Cyberspace Administration of China	2023.02.22	2023.06.01	部门规章 Departmental Regulations
8	《个人信息出境标准合同备案指南（第一版）》 "Guidelines for Filing Standard Contract for Outbound Transfer of Personal Information (First Edition)"	国家互联网信息办公室 Cyberspace Administration of China	2023.05.30	2023.05.30	规范性文件 Normative Document
9	《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》 “Implementation Guidelines on the Standard Contract for Cross-boundary	国家互联网信息办公室, 香港创新科技及工业局 Cyberspace Administration of China, Hong Kong	2023.12.10	2023.12.10	地方法规 Local Regulations

序号 No.	文件名称 Name of Document	发文机关 Issuing Body	发文时间 Issuing Date	生效时间 Effective Date	效力层级 Level of Strength
	Flow of Personal Information Within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong)"	Innovation and Technology Commission			
10	《个人信息保护认证实施规则》 "Implementation Rules for Personal Information Protection Certification"	国家互联网信息办公室,国家市场监督管理总局 Cyberspace Administration of China, State Administration for Market Regulation	2022.11.04	2022.11.04	规范性文件 Normative Document
11	《规范和促进数据跨境流动规定（征求意见稿）》 "Provisions on Regulating and Promoting Cross-border Flow of Data (Exposure Draft)"	国家互联网信息办公室 Cyberspace Administration of China	2023.09.28	——	部门规章 Departmental Regulations
12	《网络安全标准实践指南—个人信息跨境处理活动安全认证规范 V2.0》 V2.0》 "Guidelines for Cybersecurity Standard Practice - Security Certification Specification for Cross-border Processing Activities of Personal Information V2.0"	全国信息安全标准化技术委员会 National Information Security Standardization Technical Committee	2022.12.16	2022.12.16	标准相关技术文件 Standard-related Technical Document

序号 No.	文件名称 Name of Document	发文机关 Issuing Body	发文时间 Issuing Date	生效时间 Effective Date	效力层级 Level of Strength
13	《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》 "Guidelines for Cybersecurity Standard Practice - Security Certification Specification for Cross-border Processing Activities of Personal Information"	全国信息安全标准化技术委员会 National Information Security Standardization Technical Committee	2022.06.24	2022.06.24	标准相关技术文件 Standard-related Technical Document
14	《网络数据安全管理条例（征求意见稿）》 "Regulations on Network Data Security Management (Draft for Comments)"	国家互联网信息办公室 Cyberspace Administration of China	2021.11.14	——	规范性文件 Normative Document
15	《信息安全技术 重要数据识别指南（征求意见稿）》 "Information Security Technology - Guidelines for Identification of Important Data (Draft for Comments)"	全国信息安全标准化技术委员会 National Information Security Standardization Technical Committee	2022.01.13	——	推荐性国标 Recommended National Standard

作者

Authors

上海段和段律师事务所

Duan & Duan Law Firm

编写成员（Members）：

- 高亚平 Vera GAO | 权益合伙人、高级合伙人、香港注册外地律师、DPO 授权讲师 Equity Partner, Senior Partner, HK Registered Foreign Lawyer, DPO Accredited Trainer by EXIN
- 周梦 Zoe ZHOU | 合伙人、DPO 授权讲师 Partner, DPO Accredited Trainer by EXIN
- 纪倩 Joyce JI | 律师 Associate
- 徐晶 Icey XU | 律师 Associate

上海数据集团有限公司

Shanghai Data Group Co., Ltd.

编写成员（Members）：

- 高瑞鑫 Ruixin GAO | 数据安全合规专家、数据跨境小组成员 EXIN-DPO、CCRC-DCO、ESI-CDO Data security compliance expert, member of data cross-border team
- 袁旻旭 Minxu YUAN | 投资管理专家、数据跨境小组牵头人 Investment management expert, leader of data cross-border team
- 陈茜 Qian CHEN | 法律事务专家、数据跨境小组成员 Legal affairs expert, member of data cross-border team

上海段和段律师事务所

Duan & Duan Law Firm

段和段律师事务所 1993 年在上海成立，是一家拥有 30 多家境内外分所/办公室的综合性和国际化律所。段和段秉承法律至上、依法治国和客户为先、回馈社会的基本准则，走出了中国律所国际化、专业化、规模化的成功发展之路。段和段数据团队是国内数据合规领域特色法律服务的创新开拓者与引领者，在数据出境、IPO 数据合规、数据合规管理体系搭建等领域均具备独特资源优势与丰富业务经验。

Established in 1993 in Shanghai, Duan & Duan Law Firm is a comprehensive and international law firm with more than 30 domestic and international branches/offices. Adhering to the basic principles of legal supremacy, ruling the country according to the law, putting clients first and contributing to the society, Duan & Duan has walked out of the road of successful development of Chinese law firms in internationalization, specialization and scale. The Duan & Duan Data Team is an innovator and key player in providing unique legal services for data compliance in China, with unique resource advantages and rich business experience in the field of cross-border data transfer, IPO data compliance, and data compliance management system construction, etc.

上海数据集团有限公司

Shanghai Data Group Co., Ltd.

上海数据集团有限公司是以数据为核心业务的具有功能保障属性的市场竞争类市属一级国企。作为上海市公共数据授权运营主体和城市一体化大数据资源基础治理的支撑主体，以推进数据要素市场建设、激发数据要素潜能、保障数据安全为战略使命，以促进公共数据、社会数据、个人数据融合开发利用为主责主业，聚焦数字产业化、产业数字化和推动数据产业生态发展，践行“数据治理体系共建者、数据资源体系开拓者、数字经济发展引领者、数字政府建设推动者、国际数据合作先行者”的责任担当，致力于成为世界一流的数据要素型企业。

Shanghai Data Group Co., Ltd. is a first-level state-owned enterprise with data as its core business. As the authorized operating entity of Shanghai's public data and the supporting entity for the basic governance of urban integrated big data resources, it takes promoting the construction of the data element market, stimulating the potential of data elements, and ensuring data security as its strategic mission to promote public data, social data, and personal data. Integrated development and utilization are the main responsibilities and main businesses, focusing on digital industrialization, industrial digitization and promoting the ecological development of the data industry, practicing "co-builder of data governance system, pioneer of data resource system, leader of digital economy development, promoter of digital government construction" As a pioneer in international data cooperation, we are committed to becoming a world-class data element-based enterprise.

段和段律所事务所
Duan & Duan Law Firm

上海数据集团有限公司
Shanghai Data Group Co., Ltd.

了解更多，关注微信公众号
WeChat Official Accounts QR Code