大成 DENTONS

Data Protection and Cybersecurity Alert:

China's Security Assessment Measures for Data Export Settled at Long Last, Countdown to Implementation on September 1st

July 2022

This document is not designed to provide legal or other advice and you should not take, or refrain from taking, action based on its content. For any specific questions, please contact the partners below.

Contact:

Ken Dai
Partner
Shanghai Office
Tel: 021 - 5878 1965
Email: jianmin.dai@dentons.cn

Jet Deng
Partner
Beijing Office
Tel: 010 - 5813 7038
Email: zhisong.deng@dentons.cn

Following the release of the *Guidelines for Cybersecurity Standards Practices - Security Certification Specifications for Cross-Border Processing of Personal Information* (《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》in Chinese) on June 24, 2022, and the *Provisions on Standard Contract for Cross-border Transfer of Personal Information (Draft for Comments)* (《个人信息出境标准合同规定（征求意见稿）》in Chinese) along with the *Standard Contract for Cross-border Transfer of Personal Information* ("**Standard Contract**") on June 30, 2022, the Cyberspace Administration of China ("**CAC**") formally issued the *Measures for the Security Assessment of Data Cross-border Transfer* (《数据出境安全评估办法》in Chinese, "**Assessment Measures**") at long last on July 7, 2022, following its draft published on October 29, 2021.

The Assessment Measures will come into force on September 1, 2022, the first anniversary of the implementation of the *Data Security Law of the People's Republic of China*. With less than two months left, it is highly recommended that the relevant enterprises should evaluate the application of the security assessment and get well prepared for its implementation, if necessary.

Notably, if the data export activities that have been carried out before the implementation of the Assessment Measures do not conform to the provisions thereunder, rectification shall be completed within 6 months from September 1, 2022.

This alert will introduce the Assessment Measures from a practical perspective for reference by enterprises, especially multinationals, with the needs for cross-border transfer of important data and a large amount of personal information.

I. Application Scope

The Assessment Measures largely maintains the substantive provisions regarding the application scope in its draft, with further clarification on the thresholds for personal information.

Specifically, on the one hand, the following two types of data handlers shall always apply for security assessment when providing overseas important data and/or personal information collected and generated in the course of operations within the territory of mainland China (hereinafter, "**China**", excluding Hong Kong, Macau and Taiwan):

1) critical information infrastructure operators ("**CIIOs**"); and

2) personal information handlers that have processed personal information of more than 1 million individuals.

On the other hand, for non-CIIOs that have processed personal information of less than 1 million individuals, security assessment shall also be applied for if any of the following conditions is met:

1) providing **important data** abroad;

2) providing **personal information** of more than 100,000 individuals accumulatively since January

1st of the preceding year abroad; or

3) providing **sensitive personal information** of more than 10,000 individuals accumulatively since January 1st of the preceding year abroad.

Such application scope corresponds to that of the Standard Contract. That means, for non-CIIOs that have processed personal information of less than 1 million individuals, if none of the above conditions is met, the approach of Standard Contract could be adopted for cross-border transfer of personal information, without the need to apply for security assessment. Otherwise, security assessment will be triggered.

II. Self-assessment

Before applying for security assessment, a self-assessment of the risks of data export shall be conducted first, focusing on the following aspects:

1) the legality, legitimacy, and necessity of the purpose, scope, and method of data export and of the processing activities of overseas recipient;

2) the amount, scope, type and sensitivity of the data to be exported, the risks that the data export may pose to national security, public interest, and the legitimate rights and interests of individuals or organizations;

3) whether the responsibility and obligations undertaken by the overseas recipient, as well as its management and technical measures and capacity to fulfill the responsibility and obligations can ensure the security of the data to be exported;

4) the risks of data being tampered with, destroyed, leaked, lost, transferred, or illegally obtained or used during or after data export, and whether the channels for individuals to exercise the rights and interests of personal information are available, etc.;

5) whether the data export related contract or other documents with legal force (collectively, "**legal document**") to be concluded with the overseas recipient fully specifies data security protection responsibilities and obligations; and

6) other matters that may affect the security of data export.

III. Application for Security Assessment

According to the Assessment Measures, the following materials shall be submitted for the application for security assessment:

1) a written application;

2) the report of self-assessment on the risks of data export;

3) the legal document to be concluded between the data handler and the overseas recipient; and

4) other materials required for the security assessment.

It is unclear what shall be included in the written application. We understand that a template may be issued by the competent authorities next for efficiency. With respect to the report of self-assessment, for personal information export, it is supposed that the report of personal information protection impact assessment could be submitted instead.

As for the legal document, the Assessment Measures requires that at least the following matters shall be included:

1) the purpose, method and scope of data export, the purpose and method of data processing by the overseas recipient;

2) the location and duration of data storage outside China, as well as the measures to handle the data exported after the retention period expires, the agreed purpose is completed, or the contract is terminated;

3) the binding provisions that restrict the overseas recipient from transferring the exported data to other organizations or individuals;

4) the security measures that the overseas recipient should take in the event of substantial changes in actual control or scope of business, or changes in the data protection related policies and regulations and cybersecurity environment of its country or region, or other occurrence of force majeure that make it difficult to ensure data security;

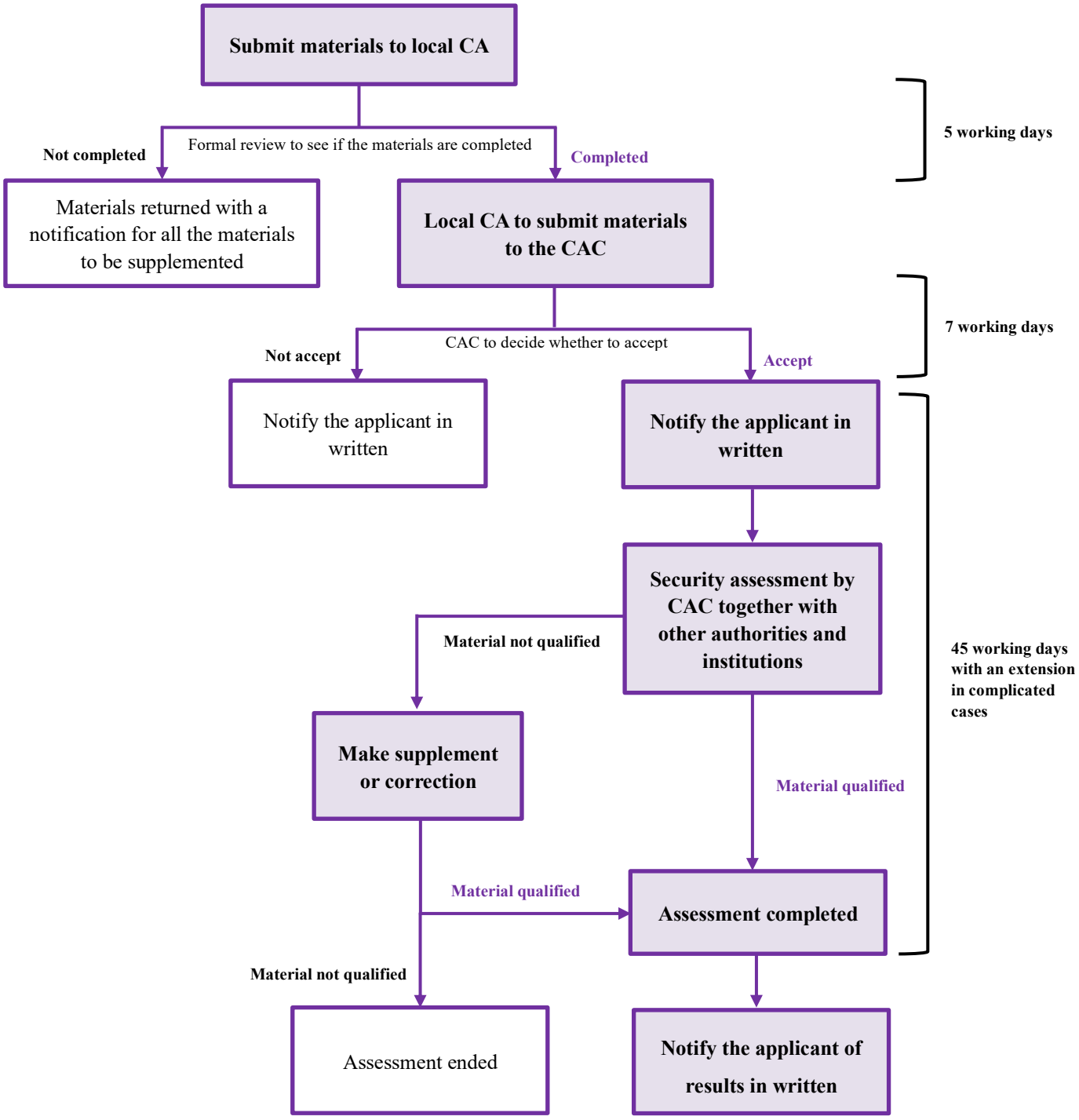
5) the remedies, liabilities and dispute resolution for breach of data security protection obligations agreed in the legal document; and

6) the requirements for proper emergency response and the ways and methods for individuals to protect their personal information rights and interest, when the data exported is at risk of being tampered with, destroyed, leaked, lost, transferred, or illegally obtained or used.

In absence of further clarification, it is supposed that, for personal information export, the Standard Contract could be used as the "legal document" to be submitted for security assessment.

IV. Assessment Authority and Timeframe

Security assessment shall be applied to the CAC through the local cyberspace administration ("**CA**") at the provincial level. The procedure and timeframe of security assessment is as below.



In addition, if the data handler has any objection to the assessment results, it can apply to the CAC for re-assessment within 15 working days upon receiving the assessment results, and the re-assessment results will be the final decision.

V. Security Assessment

Article 8 of the Assessment Measures provides the focuses of the security assessment. In particular,

the matters to be assessed in security assessment by CAC overlap with the matters of risk self-assessment to a large extent. The former mainly increases the assessment of the impact on the security of data exported of the data security protection policies and regulations and the cybersecurity environment of the country or region where the overseas recipient is located, as well as the assessment of compliance with Chinese laws, administrative regulations and departmental rules.

VI. Expiration and Re-assessment

Subject to the Assessment Measures, the assessment results will only be valid for 2 years. If it is necessary to continue the original data export activities after the expiration of the validity period, the data handler shall apply the assessment again 60 working days before the expiration. Otherwise, the data export activities shall be ceased.

Besides, during the period of validity, if there is a substantive change in data export (such as changes in the purpose, scope, method of data processing; the retention period, etc.); or there is a change in overseas laws and policies and cybersecurity environment, or in actual control of data handler and overseas recipient, that affect data security; or other circumstances that affect the security of the data exported occur, the security assessment shall be re-applied for.

VII. Looking Forward

Recently, China has intensively issued regulations and documents concerning cross-border data transfer. With the release of the guidance for certification, the draft Standard Contract and the Assessment Measures in succession, China's cross-border data transfer regime is entering into a new stage.

For enterprises, the long-standing uncertainty in this regard since the promulgation of the *Personal Information Protection Law of the People's Republic of China* and the *Data Security Law of the People's Republic of China* is being resolved, but meanwhile, great challenges are to be faced in terms of compliance work and business arrangements.

It is recommended that the relevant enterprises shall conduct a comprehensive assessment of the status quo of data export during the two-month grace period, so as to get well prepared for the implementation of the Assessment Measures. For those that do not need to apply for the security assessment, other approaches could be considered if required, as the certification mainly for intra-group transfer is close to operation, and the Standard Contact is expected to be formally issued very soon.

Appendix：Bilingual version for reference

数据出境安全评估办法	Measures for Security Assessment of Data Cross-border Transfer
第一条 为了规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，制定本办法。	**Article 1** These Measures are formulated in accordance with the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China* and other laws and regulations, with the purpose of regulating the cross-border data transfer activities, protecting the rights and interests in personal information, safeguarding national security and public benefits, and promoting the safe and free flow of data across borders.
第二条 数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息的安全评估，适用本办法。法律、行政法规另有规定的，依照其规定。	**Article 2** These Measures shall apply to the security assessment of important data and personal information collected and generated during operations within the territory of the People's Republic of China provided by data handlers to overseas. Where there are other provisions in laws and administrative regulations, such provisions shall prevail.
第三条 数据出境安全评估坚持事前评估和持续监督相结合、风险自评估与安全评估相结合，防范数据出境安全风险，保障数据依法有序自由流动。	**Article 3** The security assessment of data cross-border transfer shall adhere to the combination of ex-ante assessment and continuous supervision, and the combination of risk self-assessment and security assessment to prevent data cross-border transfer security risks and ensure the lawful, orderly and free flow of data.
第四条 数据处理者向境外提供数据，有下列情形之一的，应当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： （一）数据处理者向境外提供重要数据； （二）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； （三）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；	**Article 4** If the data cross-border transfer to be conducted by a data handler has any of the following circumstances, the data handler shall apply to the national cybersecurity administration authority via the local provincial cyberspace administration authority for security assessment: (1) the data handler provides important data overseas; (2) the operator of critical information infrastructure and data handler who has processed the

（四）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。	personal information of more than 1 million people provides personal information overseas; (3) the data handler who has provided overseas the personal information of 100,000 persons or the sensitive personal information of 10,000 persons in aggregate since January 1 of the previous year provides personal information overseas; (4) other circumstances where the security assessment of data cross-border transfer is required as prescribed by the national cyberspace administration authority.
第五条 数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项： （一）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； （二）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； （三）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； （四）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； （五）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； （六）其他可能影响数据出境安全的事项。	**Article 5** The data handlers shall, before the application for security assessment of data cross-border transfer, conduct self-assessment of the risks of data cross-border transfer, focusing on the following items: (1) legality, legitimacy and necessity of the purpose, scope, method and other aspects regarding the data cross-border transfer and the data processing of overseas recipients; (2) the scale, scope, type and sensitivity of data to be provided overseas, and the risks that data cross-border transfer may bring to national security, public interests, and the legitimate rights and interests of individuals or organizations; (3) the responsibility and obligation undertaken by the overseas recipient, as well as whether the management, technical measures and capacities to fulfill the responsibility and obligation can guarantee the security of data cross-border transfer; (4) the risks of data being tampered with, damaged, leaked, lost or transferred, or illegally obtained or used during or after the data cross-border transfer, and whether the channels for safeguarding the rights and interests of personal information are smooth; (5) whether the data cross-border transfer related contracts or other legally effective documents (hereinafter referred to as “legal documents”) to be concluded with the overseas recipients fully stipulate the responsibility and obligation of data security protection; (6) other matters that may affect the security of data cross-border transfer.

第六条 申报数据出境安全评估，应当提交以下材料： （一）申报书； （二）数据出境风险自评估报告； （三）数据处理者与境外接收方拟订立的法律文件； （四）安全评估工作需要的其他材料。	**Article 6** The following materials shall be submitted for the application for data cross-border transfer security assessment: (1) application form; (2) data cross-border transfer self-assessment report; (3) legal documents to be concluded between the data handler and the overseas recipient; (4) other materials required for security assessment.
第七条 省级网信部门应当自收到申报材料之日起 5 个工作日内完成完备性查验。申报材料齐全的，将申报材料报送国家网信部门；申报材料不齐全的，应当退回数据处理者并一次性告知需要补充的材料。 国家网信部门应当自收到申报材料之日起 7 个工作日内，确定是否受理并书面通知数据处理者。	**Article 7** The provincial cyberspace administration authority shall complete the completeness inspection within 5 working days from the date of receiving the application materials. If the application materials are complete, the application materials shall be submitted to the national cyberspace administration authority; if the application materials are incomplete, they shall be returned to the data handler and the materials that need to be supplemented shall be notified at one time. The national cyberspace administration authority shall determine whether to accept the application and notify the data handler in writing within 7 working days from the date of receiving the application materials.
第八条 数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险，主要包括以下事项： （一）数据出境的目的、范围、方式等的合法性、正当性、必要性； （二）境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求； （三）出境数据的规模、范围、种类、敏感程度，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； （四）数据安全和个人信息权益是否能够得到充分有效保障；	**Article 8** Security assessment of data cross-border transfer focus on assessing the risks that the data cross-border activities may bring to the national security, public interests, or the legitimate rights and interests of individuals and organizations, mainly including the following items: (1) the legality, legitimacy and necessity of the purpose, scope and method of data cross-border transfer; (2) the impact of data security protection policies and regulations and cybersecurity environment of the country or region where the overseas recipients are located on the safety of the data transferred across the border; whether the data protection level of the overseas recipients meet the requirements of the laws and administrative

（五）数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务； （六）遵守中国法律、行政法规、部门规章情况； （七）国家网信部门认为需要评估的其他事项。	regulations of the People's Republic of China and mandatory national standards; (3) the quantity, scope, type, and sensitivity of data transferred across the border, and the risks of data being tampered with, damaged, leaked, lost, transferred, illegally obtained or used, etc. during and after the data cross-border transfer; (4) whether data security and rights and interests of personal information can be fully and effectively guaranteed; (5) whether the legal documents to be concluded between the data handler and the overseas recipient fully stipulate the responsibility and obligation of data security protection; (6) compliance with Chinese laws, administrative regulations and departmental rules; (7) other matters where the security assessment is required according to the national cyberspace administration authority.
第九条 数据处理者应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，至少包括以下内容： （一）数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等； （二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施； （三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求； （四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、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导致难以保障数据安全时，应当采取的安全措施； （五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式； （六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。	**Article 9** The data handler shall clearly stipulate the responsibility and obligation of data security protection in the legal documents signed with overseas recipients, including at least the following contents: (1) the purpose, method and scope of transferred data of the data cross-border transfer; and the purpose, method, etc. of data processing by the overseas recipient; (2) the location of storage and retention period of data, as well as measures to be taken with the data after the retention period expires, the purpose agreed upon is completed or the legal documents are terminated; (3) binding requirements for overseas recipients to retransfer data to other organizations and individuals; (4) the security measures that the overseas recipients should take when the actual control right or business scope has changed substantially, or the data security protection policies and regulations and cybersecurity environment of the country or region where the overseas recipient is located has changed, and

	other force majeure situations has occurred so that it is difficult to ensure data security; (5) remedies, liabilities for breach of contract and dispute resolution methods for breach of data security protection obligations agreed in legal documents; (6) the requirement for proper emergency response measures and the ways and means to protect individuals' rights and interests of personal information when the data transferred across the border is tampered with, damaged, leaked, lost, transferred or illegally obtained, illegally used and encountered other risks.
第十条 国家网信部门受理申报后，根据申报情况组织国务院有关部门、省级网信部门、专门机构等进行安全评估。	**Article 10** After accepting the application, the national cyberspace administration authority shall organize relevant departments of the State Council, the provincial cyberspace administration authorities and specialized agencies, etc. to conduct security assessment according to the application.
第十一条 安全评估过程中，发现数据处理者提交的申报材料不符合要求的，国家网信部门可以要求其补充或者更正。数据处理者无正当理由不补充或者更正的，国家网信部门可以终止安全评估。 数据处理者对所提交材料的真实性负责，故意提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。	**Article 11** During the process of security assessment, if it is found that the application materials submitted by the data handler fail to meet the requirements, the national cyberspace administration authority may require them to supplement or correct the materials. If the data handler fails to supplement or correct the materials without justifiable reasons, the national cyberspace administration authority may terminate the security assessment. The data handler shall be responsible for the authenticity of the submitted materials. If they deliberately submit false materials, the assessment will be failed and be investigated for corresponding legal responsibilities according to law.
第十二条 国家网信部门应当自向数据处理者发出书面受理通知书之日起 45 个工作日内完成数据出境安全评估；情况复杂或者需要补充、更正材料的，可以适当延长并告知数据处理者预计延长的时间。 评估结果应当书面通知数据处理者。	**Article 12** The national cyberspace administration authority shall complete the data cross-border transfer security assessment within 45 working days from the date of issuing the written notice of acceptance to the data handler; If the situation is complex or the materials need to be supplemented or corrected, the said time limit may be extended appropriately and the data

	handler shall be informed of the expected extension of time. The data handler shall be notified of the assessment results in writing.
第十三条 数据处理者对评估结果有异议的，可以在收到评估结果 15 个工作日内向国家网信部门申请复评，复评结果为最终结论。	**Article 13** Data handler that has any objection to the assessment results can apply to the national cyberspace administration authority for re-assessment within 15 working days after receiving the assessment results, and the re-assessment result shall be the final decision.
第十四条 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。在有效期内出现以下情形之一的，数据处理者应当重新申报评估： （一）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； （二）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； （三）出现影响出境数据安全的其他情形。 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。	**Article 14** The validity period of the result of the data cross-border transfer security assessment is 2 years, calculated from the date of issuance of the assessment result. In case of any of the following circumstances within the validity period, the data handler shall re-apply the assessment: (1) the purpose, method, scope and type of data provided overseas, and the purpose and method of data processing by overseas recipients has changed so that it affect the security of data transferred across the border, or the overseas retention period of personal information and important data is extended; (2) the data security protection policies and regulations and cybersecurity environment in the country or region where the overseas recipients are located has changed and other force majeure situations has occurred, the actual control of the data handler or the overseas recipient has changed, the legal documents between the data handler and overseas recipients has changed, etc., so that it affect the security of data transferred across the border; (3) there are other situations that affect the security of data transferred across the border. If it is necessary to continue data cross-border transfer activities after the expiration of the validity period, the data handler shall re-apply for assessment 60 working days before the expiration of the validity period.
第十五条	**Article 15**

参与安全评估工作的相关机构和人员对在履行职责中知悉的国家秘密、个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供、非法使用。	Institutions and personnel participating in the security assessment shall keep confidential of the national security, personal privacy, personal information, trade secrets, confidential business information and other data that they come to know in the performance of their duties and shall not disclose, provide illegally to others or use them illegally.
第十六条 任何组织和个人发现数据处理者违反本办法向境外提供数据的，可以向省级以上网信部门举报。	**Article 16** Any organization or individual that finds that a data handler provides data overseas in violation of these Measures may report to the cyberspace administration authority at or above the provincial level.
第十七条 国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，应当书面通知数据处理者终止数据出境活动。数据处理者需要继续开展数据出境活动的，应当按照要求整改，整改完成后重新申报评估。	**Article 17** If the national cyberspace administration authority finds that the data cross-border transfer activities that have passed the assessment no longer meet the requirements of the security management of data cross-border transfer in the actual processing process, it shall notify the data handler in writing to terminate the data cross-border transfer activities. If the data handler needs to continue to carry out data cross-border transfer activities, it shall make rectification as required, and re-apply for assessment after rectification.
第十八条 违反本办法规定的，依据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规处理；构成犯罪的，依法追究刑事责任。	**Article 18** Those who violate the provisions of these Measures shall be punished in accordance with the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China* and other laws and regulations; where a crime is constituted, criminal liability shall be pursued in accordance with the law.
第十九条 本办法所称重要数据，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。	**Article 19** The term "important data" as mentioned in these measures refers to data that may endanger national security, economic operation, social stability, public health and safety once it is tampered with, damaged, leaked or illegally obtained or used.
第二十条 本办法自 2022 年 9 月 1 日起施行。本办法施行前已经开展的数据出境活动，不符合本办法	**Article 20** These Measures shall come into effect as of 1st September 2022. If the data cross-border transfer activities conducted before the implementation of

规定的，应当自本办法施行之日起 6 个月内完成整改。	these Measures do not comply with the provisions of these Measures, the rectification shall be completed within 6 months from the date of implementation of these Measures.

大成DENTONS

大成是世界上第一家全球多中心的律师事务所，坚持超越自我，以客户需求为中心，始终如一地提供专业、全面、及时、高效的服务，荣膺“Acritas 2015 全球顶尖 20 家精英品牌律所”称号。

我们知道，深谙本地文化对于达成交易、解决纠纷以及化解商业风险都至关重要，这促使我们深入客户业务所在的各个地区，让客户保持竞争优势。

大成--全球最大的律师事务所--全球服务团队现在更加灵活，在遍及全球 50 多个国家超过 125 个地区，为个人及公共客户提供量身定制的解决方案，满足客户在本地、本国及全球的法律服务需要。

Dentons is the world's first polycentric global law firm. A top 20 firm on the Acritas 2015 Global Elite Brand Index, the Firm is committed to challenging the status quo in delivering consistent and uncompromising quality and value in new and inventive ways.

Driven to provide clients a competitive edge, and connected to the communities where its clients want to do business, Dentons knows that understanding local cultures is crucial to successfully completing a deal, resolving a dispute or solving a business challenge. Now the world's largest law firm, Dentons' global team builds agile, tailored solutions to meet the local, national and global needs of private and public clients of any size in more than 125 locations serving 50-plus countries.

www.dentons.com.