大成 DENTONS

Data Protection Alert

China Releases New Draft Measures of Security Assessment for Data Cross-border Transfer

NOVEMBER 2021

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.

Co-Chairs

Jet Deng
Partner
Beijing Office
D 010 - 5813 7038
zhisong.deng@dentons.cn

Ken Dai
Partner
Shanghai Office
D 021 - 5878 1965
jianmin.dai@dentons.cn

On 29 October, 2021, the Cyberspace Administration of China ("**CAC**") released the *Data Export Security Assessment Measures (Draft for Comments)* (《数据出境安全评估办法（征求意见稿）》in Chinese, "**Draft Measures**") to solicit public comments. Cross-border transfer of data has always been one of the most concerned issues for entities operating in China, especially for multinationals. As the third try of the CAC since its release of the other two draft measures respectively in 2017 and 2019, this latest version shall be paid great attention to. This alert will introduce how the Draft Measures interacts with the current data protection legislations and elaborate key highlights for kind reference.

I. Who Are Caught Under the Draft Measures

According to the Draft Measures, the following two types of subjects shall always apply for security assessment when providing overseas important data and/or personal information:

- critical information infrastructure operators; and
- personal information handlers that have processed personal information of more than 1 million individuals.

In addition, security assessment shall also be applied if the following data will be transferred or accumulatively transferred overseas, regardless of the nature of the data hander:

- important data;
- personal information of more than 100,000 individuals; or
- sensitive personal information of more than 10,000 individuals.

II. Self-Assessment

Before applying to the CAC through its local counterpart for security assessment, a self-assessment shall be conducted at first.

The key points of the self-assessment include the following:

- the legality, justifiability, and necessity of the purpose, scope, and method of data export and of the processing activities of overseas recipient;
- the amount, scope, type and sensitivity of the data to be exported, the risk that the data export may pose to national security, public interest, and the legitimate rights and interests of individuals or organizations;
- whether the management and technical measures and capacity of the data handler in the data transfer process can prevent the risk of data leakage, destruction, etc.;
- whether the responsibility and obligations undertaken by the overseas recipient, as well as the management and technical measures and capacity to fulfill the responsibility and obligations can ensure the security of the data to be exported;
- the risk of data leakage, destruction, tampering, abuse, etc. after the export and retransfer, and whether the channels for individuals to safeguard the rights and interests of personal information are available, etc.; and
- whether the data export-related contract concluded with the overseas recipient fully specifies data security protection responsibilities and obligations.

III. Initiating a Security Assessment

Entities need to prepare the following materials for an application for a security assessment:

- a written application (the template of which may be issued by authorities);
- the self-assessment report on the risks of data export;
- the contract or other legally binding documents concluded between the data handler and the overseas recipient; and
- other materials required for the security assessment.

Specifically, the contract entered into by the data handler and the overseas recipient to fully provide the data security protection responsibilities and obligations should include, but not be limited to, the following items:

- the purpose, method and scope of data export, the purpose and method of data processing by the overseas recipient;
- 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;
- the binding provisions that restrict the overseas recipient from transferring the exported data to other organizations or individuals;
- 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 legal environment of the country or region that make it difficult to ensure data security;
- the liability for breach of data security protection obligations, and the binding and enforceable dispute resolution provisions; and
- the smooth communication channels and appropriate emergency response in the event of data leakage and other risks to protect the data subjects' rights and interests.

IV. Focuses of the Security Assessment

The data export security assessment focuses on assessing the risks that the data export activities may pose to national security, public interests, and the legitimate rights and interests of individuals or organizations, mainly including the following matters:

- the legality, justifiability, and necessity of the purpose, scope, and method of data export;
- the impact of the data security protection policies and regulations and network security environment of the country or region where the overseas recipient is located on the security of the exported data; whether the level of data protection of the overseas recipient meets the requirements of the laws, administrative regulations and mandatory national standards of China;
- the quantity, scope, type and sensitivity of the data to be exported, the risks of leakage, tampering, loss, destruction, transfer or illegal access, illegal use, etc. in and after the export;
- whether the data security and the rights and interests in personal information can be fully and effectively protected;
- whether the contract between the data handler and the overseas recipient fully specifies the responsibilities and obligations of data security protection;
- compliance with Chinese laws, administrative regulations and departmental rules; and
- other matters that the CAC considers necessary to assess.

V. Timeframe and Authorities

Security assessment shall be applied to the CAC through the local cyberspace administration at the provincial level.

The CAC within 7 working days from the date of receipt of the application materials will determine whether to accept the assessment and give feedback in the form of a written notice on the acceptance results.

After accepting the application, the CAC will organize the competent sectoral authorities, relevant departments of the State Council, provincial cyberspace administrations, and specialized agencies to conduct security assessment.

The CAC will complete the data export security assessment within 45 working days from the date of issuing the written notice of acceptance; if the situation is complex or additional materials are required, the above time limit can be extended appropriately, but generally not exceeding 60 working days.

VI. Expiration and Re-assessment

The assessment result is only 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.

During the period of validity, the data handler shall re-apply for assessment if any of the following circumstances occurs:

- the purpose, method, and scope of exporting data, the type of data exported and the purpose and method of processing data by the overseas recipient change, or the period of retention of personal information and important data outside China is extended;
- the legal environment of the country or region where the overseas recipient is located changes, the actual control of the data handler or the overseas recipient changes, or the contract between the data handler and the overseas recipient changes that may affect the security of the data exported;
- the emergence of other circumstances affecting the security of the data exported.

VII. Looking Forward

Published three days before the effective date of the Personal Information Protection Law ("**PIPL**"), the Draft Measures intends to supplement the current legislations and provides practical guidance for data cross-border transfer. With the implementation of the Data Security Law and the PIPL, it is noteworthy that the violations against the rules concerning data cross-border transfer may incur heavy penalties, such as a fine up to CNY 50 million (about USD 7,820,000) or not more than 5% of the entity's turnover of the previous year, and among other things, the person in charge may also be fined and prohibited from holding key positions within a certain period of time. It is therefore recommended to pay close attention to the development of the Draft Measures and conduct data cross-border transfer cautiously in practice.

Appendix

数据出境安全评估办法（征求意见稿）	**The Measures for the Security Assessment of Data Export (Exposure Draft)**
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: The present Measures are enacted 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, in order to regulate the activities of outbound data, protect the rights and interests in personal information, safeguard national security and social and public interests as well as promote 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依法应当进行安全评估的个人信息，应当按照本办法的规定进行安全评估；法律、行政法规另有规定的，依照其规定。	Article 2: Unless otherwise provided for in laws and administrative regulations, data processors are required to conduct security assessment according to these Measures when they provide overseas important data collected and generated during their operation within the territory of the People's Republic of China and personal information that shall be subject to security assessment according to law.
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: It is imperative to conduct security assessment for the outbound data under the principle of combining ex ante assessment and continuous inspection as well as combining risk self-assessment and security assessment, so as to prevent security risks from the outbound data and ensure the orderly and free flow of data in accordance with the law.
第四条 数据处理者向境外提供数据，符合以下情形之一的，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）关键信息基础设施的运营者收集和产生的个人信息和重要数据； （二）出境数据中包含重要数据； （三）处理个人信息达到一百万人的个人信息处理者向境外提供个人信息； （四）累计向境外提供超过十万人以上个人信息或者一万人以上敏感个人信息； （五）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。	Article 4: To provide data abroad, a data processor falling under any of the following circumstances shall, through the local cyberspace administration at the provincial level, apply to the Cyberspace Administration of China ("CAC") for security assessment of outbound data. (I) where the outbound data are personal information and important data collected and generated by operators of critical information infrastructure; (II) where the outbound data contains important data; (III) where a personal information processor that has processed personal information of more than one million people provides personal information overseas; (IV) where the personal information of more than 100,000 people or sensitive personal information of more than 10,000 people are transferred overseas accumulatively; or (V) other circumstances under which security assessment of outbound data is required as prescribed by the CAC.

第五条 数据处理者在向境外提供数据前，应事先开展数据出境风险自评估，重点评估以下事项： （一）数据出境及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）出境数据的数量、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）数据处理者在数据转移环节的管理和技术措施、能力等能否防范数据泄露、毁损等风险； （四）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； （五）数据出境和再转移后泄露、毁损、篡改、滥用等的风险，个人维护个人信息权益的渠道是否通畅等； （六）与境外接收方订立的数据出境相关合同是否充分约定了数据安全保护责任义务。	Article 5: Prior to providing data abroad, a data processor shall conduct self-assessment of the risks of outbound data, with emphasis on the assessment of the following matters: (I) legality, appropriateness and necessity of the outbound data and the purpose, scope and method of the overseas recipient's processing of the data; (II) the quantity, scope, type and sensitivity of the outbound data; risks to national security, public interests, and the legitimate rights and interests of individuals or organizations that may arise from the outbound data; (III) whether the management, technical measures and capabilities of the data processor in the data transfer link can prevent data leakage, damage and other risks; (IV) the responsibilities and obligations that the overseas recipient undertakes to assume, and whether the management, technical measures and ability to perform the responsibilities and obligations can ensure the security of the outbound data; (V) risks of leakage, damage, tampering and abuse of data after the data is transmitted abroad and further transferred, and whether the channels for individuals to maintain their rights and interests in personal information are unblocked; and (VI) whether the relevant contract for the outbound data concluded with the overseas recipient fully specifies the responsibilities and obligations for data security protection.
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合同或者其他具有法律效力的文件等（以下统称合同）； （四）安全评估工作需要的其他材料。	Article 6: To apply for security assessment of outbound data, the following materials shall be submitted: (I) a written application; (II) self- assessment report on risks of outbound data; (III) a contract or other legally binding documents (hereinafter collectively referred to as "the contract") to be concluded between the data processor and the overseas recipient; and (IV) Other materials required for the security assessment.
第七条 国家网信部门自收到申报材料之日起七个工作日内，确定是否受理评估并以书面通知形式反馈受理结果。	Article 7: The CAC shall, within seven working days from the date of receipt of the application materials, determine whether to accept the assessment application, and give feedback on the acceptance results in the form of a written notice.

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及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、行政法规规定和强制性国家标准的要求； （三）出境数据的数量、范围、种类、敏感程度，出境中和出境后泄露、篡改、丢失、破坏、转移或者被非法获取、非法利用等风险； （四）数据安全和个人信息权益是否能够得到充分有效保障； （五）数据处理者与境外接收方订立的合同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。	Article 8: Security assessment of outbound data shall focus on the assessment of the risks to national security, public interests, and the legitimate rights and interests of individuals or organizations caused by the outbound data, mainly including the following matters: (I) Legality, legitimacy and necessity of the purpose, scope and method of transmitting the data abroad; (II) The impact of the policies and regulations on data security protection and the network security environment of the country or region where the overseas recipient is located on the security of the outbound data; and whether the data protection level of the overseas recipient meets the requirements of the laws and administrative regulations of the People's Republic of China and the mandatory national standards; (III) The quantity, scope, type and sensitivity of the outbound data, and the risks of leakage, tampering, loss, damage, transfer, or of illegal acquisition or illegal use of such data when leaving the country or thereafter; (IV) Whether the data security and the rights and interests in personal information can be adequately and effectively protected; (V) Whether the contract between the data processor and the overseas recipient has made sufficient provisions on the responsibilities and obligations for data security protection; (VI) Compliance with Chinese laws, administrative regulations, and departmental rules; and (VII) Other matters that the CAC considers necessary to be assessed.

第九条 数据处理者与境外接收方订立的合同充分约定数据安全保护责任义务，应当包括但不限于以下内容： （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、完成约定目的或者合同终止后出境数据的处理措施； （三）限制境外接收方将出境数据再转移给其他组织、个人的约束条款； （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、地区法律环境发生变化导致难以保障数据安全时，应当采取的安全措施； （五）违反数据安全保护义务的违约责任和具有约束力且可执行的争议解决条款； （六）发生数据泄露等风险时，妥善开展应急处置，并保障个人维护个人信息权益的通畅渠道。	Article 9: The contract between a data processor and an overseas recipient, which fully provides for the responsibilities and obligations for data security protection, shall include but not be limited to the following: (I) The purpose and method of transmitting the data abroad and the scope of the outbound data; and the purpose and method of data processing by the overseas recipient; (II) The place and duration of overseas storage of the data, as well as the measures to deal with the data after the storage period expires, the purpose agreed upon is completed or the contract is terminated; (III) restrictive clauses restricting the overseas recipient from re-transferring the data transmitted abroad to other organizations or individuals; (IV) Security measures that shall be taken in case of any substantial change in the actual control right or business scope of the overseas recipient, or any change in the legal environment of the country or region where the overseas recipient is located, which makes it difficult to guarantee data security; (V) Liability for breach of the data security protection obligation, and binding and enforceable dispute resolution clauses; and (VI) Properly carrying out emergency response in case of data leakage and other risks and ensuring the smooth channels for individuals to safeguard their personal information rights and interests.
第十条 国家网信部门受理申报后，组织行业主管部门、国务院有关部门、省级网信部门、专门机构等进行安全评估。 涉及重要数据出境的，国家网信部门征求相关行业主管部门意见。	Article 10: After accepting an application, the CAC shall organize the competent authority of the industry concerned, relevant departments of the State Council, the cyberspace administration at the provincial level and specialized agencies to conduct security assessment. For any outbound data involving important data, the CAC shall seek opinions from the competent authority of the industry concerned.
第十一条 国家网信部门自出具书面受理通知书之日起四十五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材料的，可以适当延长，但一般不超过六十个工作日。 评估结果以书面形式通知数据处理者。	Article 11: The CAC shall complete security assessment of outbound data within 45 working days commencing from the date of issuing the written notice of acceptance; if the circumstance is complex or supplementary materials are required, the said time limit may be extended appropriately, but generally shall not exceed 60 working days. The data processor shall be notified of the assessment result in writing.

第十二条 数据出境评估结果有效期二年。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、类型和境外接收方处理数据的用途、方式发生变化，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法律环境发生变化，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合同变更等可能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，需要继续开展原数据出境活动的，数据处理者应当在有效期届满六十个工作日前重新申报评估。 未按本条规定重新申报评估的，应当停止数据出境活动。	Article 12: The outbound data assessment result is valid for two years. If any of the following circumstances occurs during the validity period, the data processor shall re-apply for assessment: (I) Any change occurs to the purpose, method, scope, or type of outbound data, or the use or method of data processing by the overseas recipient, or the period for overseas storage of personal information and important data is extended; (II) Any change in the legal environment of the country or region where the overseas recipient is located, any change in the actual control of the data processor or the overseas recipient, or any change in the contract between the data processor and the overseas recipient that may affect the security of the outbound data; (III) Other circumstances affecting the security of outbound data. If it is necessary to continue the outbound provision of the original data upon expiration of the validity period, the data processor shall apply for assessment again 60 working days before expiration. Where no new application is filed for assessment under the provisions of this Article, relevant data outbound activities shall be ceased.
第十三条　数据处理者应当按照本办法的规定提交评估材料，材料不齐全或者不符合要求的，应当及时补充或者更正，拒不补充或者更正的，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。	Article 13: The data processor shall submit the assessment materials in accordance with the provisions of the present Measures. In case the materials are incomplete or not in compliance with the requirements, it shall make supplements or corrections in a timely manner. If it refuses to make supplements or corrections, the CAC may terminate the security assessment; the data processor shall be responsible for the authenticity of the materials submitted, and if it intentionally submits false materials, it shall be deemed to have failed the assessment.
第十四条 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。	Article 14: Relevant agencies and personnel participating in the security assessment shall, in accordance with the law, keep confidential the state secrets, personal privacy, personal information, trade secrets, confidential business information and other data learned in the performance of their duties, and shall not disclose or illegally provide such information to others.
第十五条 任何组织和个人发现数据处理者未按照本办法规定进行评估向境外提供数据的，可以向省级以上网信部门投诉、举报。	Article 15: Organizations or individuals who find that any data processor provides data abroad without an assessment in accordance with the present Measures may complain or report to the cyberspace administrations at the provincial level or above.

第十六条　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，应当撤销评估结果并书面通知数据处理者，数据处理者应当终止数据出境活动。需要继续开展数据出境活动的，数据处理者应当按照要求进行整改，并在整改完成后重新申报评估。	Article 16: Where the CAC finds that any outbound data which has passed the assessment no longer meets the security management requirements for outbound data in the actual process, it shall cancel the assessment results and notify the data processor in writing of the same. The data processor shall terminate the outbound data activities. If it is necessary to continue such activities, the data processor shall make rectifications as required and apply for an assessment anew after completing the rectifications.
第十七条 违反本办法规定的，依照《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》等法律法规的规定处理；构成犯罪的，依法追究刑事责任。	Article 17: Any violation of the present Measures shall be punished in accordance with the laws and regulations such as 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; if a crime is constituted, criminal liability shall be pursued in accordance with the law.
第十八条 本办法自 年 月 日起施行。	Article 18: The present Measures shall come into force as of MM/DD/YY.

ABOUT DENTONS

Dentons is the world's largest law firm, connecting top-tier talent to the world's challenges and opportunities with 20,000 professionals including 12,000 lawyers, in more than 200 locations, in more than 80 countries. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and award-winning client service challenge the status quo to advance client interests.

dentons.com

CSBrand-74201-Data Protection Alert in China brochure — 18/11/2021