## China Eases Regulation of Outbound Data Flow
## Fact Sheet on the Provisions to Promote and Regulate Cross-Border Data Flow

*By VTeam*

On March 22, 2024, the Cyberspace Administration of China ("***CAC***"), China's data protection regulator, released the finalized Provisions on Regulating and Promoting Cross-Border Data Flows ("***Provisions***"). To everyone's surprise, the long-awaited Provisions were actually approved by the CAC on November 28th, 2023. The Provisions take effect immediately upon issuance. Coincidentally, the China Development Forum will be held in Beijing on March 24 and 25, 2024 and will be attended by more than 800 CEOs of global industry giants.

**Regulatory Mechanism**

The Provisions does not change the existing regulatory mechanism of outbound data transfer. That is, data processors outbound transferring data should apply for the CAC's security assessment ("***Security Assessment***"), or file for record with the provincial office of the CAC the Chinese standard contractual clauses they sign with the foreign data recipients ("***CN SCC Filing***"), or obtain the personal information protection certification("***Certification***"). Comparing with the threshold prior to the Provisions, the Provisions sets it higher, which will reduce the administrative procedural burden of the MNC data processors in outbound transferring data and personal information.

Along with the publication of the Provisions, the CAC simultaneously released the updated guidelines for the Security Assessment and the CN SCC Filing pursuant to the Provisions and is offering some apparent convenience to help data processors navigate the regulatory mechanism. For example, the CAC is launching online the Data Outbound Transfer Reporting System at https://sjcj.cac.gov.cn. Data processors applying to Security Assessment and CN SCC Filing can now submit their applications online. Data processors applying for Certification can go to the Personal Information Protection Certification Administration System at https://data.isccc.gov.cn. However, the CAC will maintain the offline submission channels at its provincial offices for submissions by the Critical Information Infrastructure Operators ("***CIIOs***") or by other applicants for whom the online submission is not appropriate. It remains to be seen which applicants will fall into this category.

In addition, the CAC also announces the inquiry channels for the regulatory mechanism. At the central authority level, for Security Assessment, the consultation hotline is (8610) 5562 7135 and the inquiry email address is sjcj@cac.gov.cn; for CN SCC Filing, the consultation hotline (8610) 5562 7565 and the inquiry email address bzht@cac.gov.cn; for Certification, (8610) 8226 1100 and data@isccc.gov.cn. Provincial channels will remain in place. The same inquiry channels will also take whistleblower reports. Since release of the draft of the Provisions, there were difficulties getting responses from the query channels. It would be nice if they will work to provide responses again.

**Clarifications and Exemptions**

The Provisions clarify some key issues in the regulatory mechanism and define exemptions from such regulatory mechanism. These key issues and exemptions resolve many complaints about uncertainties in the regulatory mechanism. Although the outcome of the Provisions remains to be seen, the government's intention to make easier the data outbound transfer in the normal international business operations of the MNCs is clear.

The exemptions in the Provisions include:

(1) If there is no individual notice or public announcement by the competent regulatory authorities or local governments defining the data outbound transferred by a data processor as important data, the data processor should not be required to conduct the Security Assessment. However, this is subject to the data processor fulfilling its legal obligations to identify and report the important data it processes in accordance with the relevant rules, if any;

(2) A data processor needs not to go through the regulatory mechanism for the data collected or generated from its business activities of international trade, international logistics, academic cooperation, transnational manufacturing, and marketing and promotion, if there is no personal information or important data in such data;

(3) A data processor needs not to go through the regulatory mechanism when it "re-exports" personal information generated or collected outside China and imported into China for processing, as long as no personal information of data subjects in China and no important data are comingled into such imported data in the processing;

(4) A data processor needs not to go through the regulatory mechanism if it is *truly necessary* to outbound transfer the personal information (a) of the individual parties to the contracts for the purpose of entering into and performing the contracts. Cited examples of such contracts include cross-border eCommerce, cross-border mail and courier delivery, cross-border payment wiring, cross-border accounts opening, air-tickets and hotel booking, visa processing, tests/examination service, or (b) of its employees for cross-border human resource management in accordance with the labor rules and policies formulated under the Chinese law and the collective labor contracts concluded with the employees, or (c) to protect the life, the health and the property safety of the individuals in emergencies; and

(5) A data processor that is not a CIIO need not to go through the regulatory mechanism if it outbound transfers personal information of less than 100,000 data subjects (after removing duplicates) in China from January 1st of the year, as long as such outbound transferred personal information does not contain sensitive personal information and important data.

**Reduced Scope of the Regulatory Mechanism**

The Provisions narrow the scenarios in which the Security Assessment is applicable. A data processor is only required to conduct the Security Assessment if (a) it is a CIIO and it outbound transfers personal information or important data; or (b) although it is not a CIIO, from January 1st of the year and after duplicates are removed, it outbound transfers (i) important data, or (ii) personal information (other than sensitive personal information) of more than one million data subjects in China, or (iii) sensitive personal information of more than 10,000 (inclusive) data subjects in China. The number of data subjects for such a purpose should be exclusive of the number of data subjects in the exempted scenarios.

A data processor should apply for the CN SCC Filing or obtain the Certification if, from January 1st of the year and after removing duplicates, it outbound transfers (a) personal information of data subjects in China more than 100,000 but less than 1,000,000, or (b) sensitive personal information of data subjects in China no more than 10,000. Similarly, the headcount for such a purpose should be exclusive of the headcount in the exempted scenarios.

**Security Assessment Extension**

According to the Provisions, the valid period or the Security Assessment cycle has been extended from two years to three years. In addition, if a data processor's outbound data transfer does not have a substantial change at the end of the three-year period, the CAC allows the data processor to apply in no later than 60 working days before the expiry of the current valid period for an extension of the valid period of the current Security Assessment approval for another three years. Such an arrangement simplifies the process and significantly reduces the burden on the MNC data processors, at least in black letters.

**Pilot Free Trade Zones**

The Pilot Free Trade Zones in China may, within the data protection framework of national classification and categorization, formulate their respective lists of data whose outbound transfer is subject to the regulatory mechanism (the "***Negative List***"). Such Negative Lists should be approved by the provincial office of the cybersecurity and informalization commission (which has the same effect as if the Negative List were approved by the provincial government) and filed with the CAC and the National Data Administration. Data not included in the Negative List of a Pilot Free Trade Zone can be outbound transferred by data processors in that Pilot Free Trade Zone without being subject to the regulatory mechanism.

**Impacts on Data Processors Having Gone Through the Regulatory Mechanism**

Given the relaxation of the Regulatory Mechanism, the CAC also provides guidance to those "model citizen" data processors who have gone through the regulatory mechanism prior to the Provisions:

- Data processors that have passed the Security Assessment may continue the outbound

transfer of the data according to the approval;

- Data processors that have failed or partially failed the Security Assessment but are not subject to the Security Assessment under the Provisions may ignore the failure and, according to the Provisions, apply for the CN SCC Filing or obtain the Certification to outbound transfer the personal information;

- Data processors that have applied for the Security Assessment or the CN SCC Filing but are not subject to those two regulatory mechanisms under the Provisions may continue with the process or withdraw their applications.

**Unchanged Data Processors Obligations**

Regardless of whether a data processor should go through the regulatory mechanism or not,

(1) When outbound transferring data, in order to ensure the data security, it should always:

a. comply with the provisions of the applicable laws and regulations;
b. comply with its obligations to maintain data security;
c. take technical and other necessary measures; and
d. report any actual or potential data security incidents to the CAC at or above the provincial level and other regulatory authorities in a timely manner and take timely remedial measures.

(2) When outbound transferring personal information, it should always:

a. duly inform the data subjects of the fact of outbound transfer;
b. obtain their separate consents where consent is the lawful ground of such outbound transfer; and
c. conduct the personal information protection impact assessment, if required by the law.

**Potential Focus and Trend**

The immediate reaction of all MNC data processors to the Provisions is that they need to revisit their prior efforts on compliance with China's data outbound transfer regulatory mechanism. For MNC data processors who are lucky pioneers in the compliance and have already passed the regulatory mechanism without any reservation by the CAC, they need to rethink about their compliance strategies and efforts in practice according to the new thresholds under the Provisions. For those pioneers which failed or partially failed the regulatory mechanism, they need to immediately assess their failure and determine whether the failed outbound transfers are qualified for a second chance under the Provisions. If so, they can follow the practice in the next sentence. For those who are preparing for the compliance in accordance with the threshold prior to the Provisions, they need to immediately assess whether they need to make changes to the submissions in preparation to align with the Provisions and the new guidelines, or, luckily enough, whether they are exempt from the regulatory mechanism.

The Provisions requires that all provincial offices of the CAC should (a) strengthen their guidance and supervision on data outbound transfer, (b) improve and optimize the Security Assessment policy and process, (c) strengthen the whole fields and the whole process supervision. It is reasonable to expect that the CAC will make more efforts to enforce and punish violations after relaxing the administrative procedures. Relevantly or not, the focus of the 3.15 event (i.e., the consumer protection event) has already shifted to personal information violations. Therefore, MNC data processors in China should take measures to comply with the relaxed procedures and improve their important data and privacy compliance in daily operations.

The Provisions sends a clear message to the industrial regulatory authorities and local governments that they need to take the initiative to identify and determine the important data, or, otherwise, the data processors have no obligation to treat the data they outbound transfer as important data if they do not receive notices or public announcements from the aforesaid authorities. The underlined statement is that it is the responsibility and liability of the industrial regulatory authorities and local governments if important data that should have been subject to the regulatory mechanism is outbound transferred without going through the regulatory mechanism. Therefore, it is expected that the industry regulatory authorities and the local governments may hastily release their respective important data determination policies and catalogues. The potential impact of such a rush to determine important data deserves further attention.

Given that each Pilot Free Trade Zone may have its own Negative List under the Provisions, an MNC data processor may wish to track the formulation of such Negative Lists for a smart and personalized forum-shopping strategy based on its overall data and personal information outbound transfer needs or the specific data and personal information outbound transfer needs of its business unites or divisions.

* * *

*Should you have questions about any of the above issues or need legal support in the above area, you are welcome to contact us. We offer 30-minutes complimentary conference time with new clients using our services.*

*Disclaimer. This article does not represent legal advice of our team on the relevant issues. If you need legal advice or other expert advice, please seek assistance from professional legal counsel.*

**Annex 1**

## 《促进和规范数据跨境流动规定》
## Provisions on Promoting and Regulating Cross-Border Data Flows

第一条 为了保障数据安全，保护个人信息权益，促进数据依法有序自由流动，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，对于数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度的施行，制定本规定。

Article 1 For the purpose of safeguarding data security, protecting personal information rights and interests, and promoting the lawful, orderly and free flow of data, the Provisions are formulated to implement the data outbound regulatory mechanism, including the security assessment of the outbound data transfer ("Security Assessment"), the standard contract for the outbound transfer of personal information ("Standard Contract"), and the personal information protection certification ("Certification"), in accordance with the Cybersecurity Law of the People's Republic of China ("CSL"), Data Security Law of the People's Republic of China ("DSL"), Personal Information Protection Law of the People's Republic of China ("PIPL"), and other relevant laws and regulations.

第二条 数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

Article 2 Data processors shall identify and report important data in accordance with the relevant regulations. Data processors need not treat as important data any data that has not been individually notified or publicly announced as important data by the competent authorities or the local authorities and need not apply for the Security Assessment for reasons of important data.

第三条 国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的，免予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。

Article 3 Outbound transfer of the data collected and generated in the course of certain business activities, such as international trade, international logistics, academic collaboration, transnational production and manufacturing, and marketing and promotion is exempt from the Security Assessment, the Standard Contract, and the Certification, if there is no personal information or important data in such data.

第四条 数据处理者在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的，免予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。

Article 4 Outbound transfer of the data that were originally collected or generated outside of China, but later imported into China for processing, is exempt from the Security Assessment, the Standard Contract, and the Certification, if no domestic personal information or important data are comingled into such imported data in its processing in China.

第五条 数据处理者向境外提供个人信息，符合下列条件之一的，免予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：

Article 5 Data processors providing abroad personal information that meet one of the following conditions are exempt from the Security Assessment, the Standard Contract, and the Certification:

(一) 为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息的；

(i) where it is truly necessary to provide personal information abroad in order to enter into and perform contracts with counterparties of individuals, such as contracts for cross-border eCommerce, cross-border mail and courier delivery, cross-border payment wiring, cross-border account opening, air-tickets and hotel booking, visa processing, tests/examination services, etc.;

(二) 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跨境人力资源管理，确需向境外提供员工个人信息的；

(ii) when it is truly necessary to provide the personal information of employees abroad in order to carry out cross-border human resources management in accordance with the formulated labor rules and policies and the concluded collective contracts, in accordance with the law;

(三) 紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的；

(iii) when it is truly necessary to provide personal information abroad in emergency situations to protect the life, health, or property of individuals; or

(四) 关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息（不含敏感个人信息）的。

(iv) if a data processor other than a critical information infrastructure operator (“CIIO”) provides personal information (excluding sensitive personal information) of less than 100,000 individuals abroad since January 1 of the year.

前款所称向境外提供的个人信息，不包括重要数据。

The above “personal information provided abroad” shall not include important data.

第六条 自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定区内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），经省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。

Article 6 Under the national data classification and grading protection system, the Pilot Free Trade Zones may formulate their respective lists (the “Negative List”) specifying the categories of data the outbound transfer of which is subject to the Security Assessment, the Standard Contract, or the Certification. Such Negative Lists shall be approved by the provincial cybersecurity and informatization commissions and filed with the Cyberspace Administration of China (“CAC”) and the National Data Administration for record.

自由贸易试验区内数据处理者向境外提供负面清单外的数据，可以免予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。
Outbound transfer of the data that are not on the Negative Lists by data processors in the Pilot Free Trade Zones is exempt from the Security Assessment, the Standard Contract, and the Certification.

第七条 数据处理者向境外提供数据，符合下列条件之一的，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：
Article 7 Data processors providing data abroad, meeting one of the following conditions, shall be subject to the Security Assessment by filing applications with the CAC through its provincial offices:

（一） 关键信息基础设施运营者向境外提供个人信息或者重要数据；
(i) The CIIOs provide transfer personal information or important data abroad; or

（二） 关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息。
(ii) Data processors other than the CIIOs provide important data abroad, or provide personal information (excluding sensitive personal information) of more than 1,000,000 individuals or sensitive personal information of more than 10,000 individuals abroad, since January 1 of the year.

属于本规定第三条、第四条、第五条、第六条规定情形的，从其规定。
The outbound transfer falling into the circumstances provided in Article 3, Article 4, Article 5, and Article 6 hereof shall be subject to those provisions.

第八条 关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息的，应当依法与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证。
Article 8 Data processors other than the CIIOs outbound transferring personal information (excluding sensitive personal information) of more than 100,000 but less than 1,000,000 individuals or sensitive personal information of less than 10,000 individuals since January 1 of the year shall be subject to the legal requirements for the Standard Contract or the Certification.

属于本规定第三条、第四条、第五条、第六条规定情形的，从其规定。
The outbound transfer falling into the circumstances provided in Article 3, Article 4, Article 5, and Article 6 hereof shall be subject to those provisions.

第九条 通过数据出境安全评估的结果有效期为 3 年，自评估结果出具之日起计算。有效期届满，需要继续开展数据出境活动且未发生需要重新申报数据出境安全评估情形的，数据处理者可以在有效期届满前 60 个工作日内通过所在地省级网信部门向国家网信部门提出延长评估结果有效期申请。经国家网信部门批准，可以延长评估结果有效期 3 年。

Article 9 The validity period of the Security Assessment result shall be three years from the date of the Security Assessment result. Upon expiration of the validity period, if there are needs to continue outbound transferring of the data and there are no circumstances requiring re-application of the Security Assessment , the data processors may, within 60 working days before the expiration of the validity period, submit an application to the CAC through the provincial offices where it is located to extend the validity period of the Security Assessment result. Upon approval by the CAC, the validity period of the Security Assessment result may be extended for another three years.

第十条 数据处理者向境外提供个人信息的，应当按照法律、行政法规的规定履行告知、取得个人单独同意、进行个人信息保护影响评估等义务。

Article 10 In accordance with the laws and regulations, data processors who outbound transfer personal information shall fulfill obligations, such as notification, obtaining the individuals' separate consents, conducting the personal information protection impact assessment, and etc.

第十一条 数据处理者向境外提供数据的，应当遵守法律、法规的规定，履行数据安全保护义务，采取技术措施和其他必要措施，保障数据出境安全。发生或者可能发生数据安全事件的，应当采取补救措施，及时向省级以上网信部门和其他有关主管部门报告。

Article 11 Data processors providing data abroad shall comply with the provisions of the laws and the regulations, fulfill their obligations to protect data security, take technical and other necessary measures, and ensure the security of the outbound transferred data. In the event of, or potential occurrence of, data security incidents, data processors shall take remedial measures and report in a timely manner to at least the provincial offices of the CAC and other relevant competent authorities.

第十二条 各地网信部门应当加强对数据处理者数据出境活动的指导监督，健全完善数据出境安全评估制度，优化评估流程；强化事前事中事后全链条全领域监管，发现数据出境活动存在较大风险或者发生数据安全事件的，要求数据处理者进行整改，消除隐患；对拒不改正或者造成严重后果的，依法追究法律责任。

Article 12 All local offices of the CAC shall strengthen their guidance and supervision of data processors' data outbound transfer activities, improve the Security Assessment policies, optimize the Security Assessment procedures; strengthen the whole-process and whole-field supervision before, during, and after the data outbound transfer. If significant risks are identified in the data outbound transfer or if data security incidents occur, data processors shall be required to rectify the issues and eliminate the potential risks. Legal responsibilities will be pursued for those who refuse to rectify or cause serious consequences.

第十三条 2022 年 7 月 7 日公布的《数据出境安全评估办法》（国家互联网信息办公室令第 11 号）、2023 年 2 月 22 日公布的《个人信息出境标准合同办法》（国家互联网信息办公室令第 13 号）等相关规定与本规定不一致的，适用本规定。

Article 13 In the event of any inconsistencies between the Provisions and other relevant regulations, such as the Measures for the Security Assessment of the Outbound Data Transfer (Order No.11 of the CAC) released on July 7, 2022, and the Measures for the Standard Contract for the Outbound Transfer of Personal Information (Order No.13 of the CAC) released on February 22, 2023, the

Provisions shall prevail.

第十四条 本规定自公布之日起施行。
Article 14 The Provisions shall come into effect from the date of promulgation.