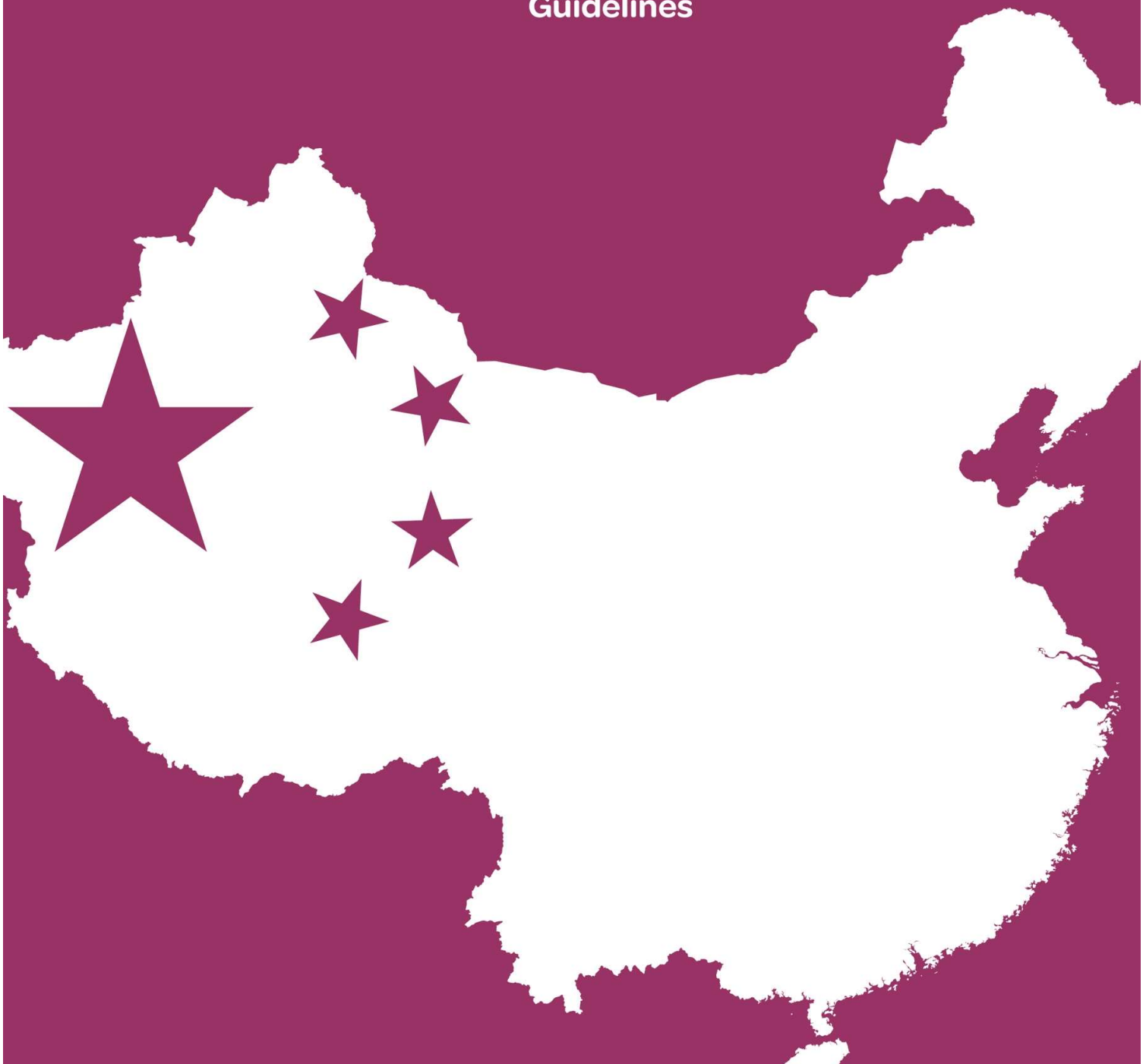
MRS Evidence Matters

CHINA CYBERSECURITY ADMINISTRATION OF CHINA (CAC)

Guidelines



China Cybersecurity Administration of China (CAC) guidelines about outbound personal data and important data to third countries Brief for Research

Background

The Cybersecurity Administration of China (CAC) published guidelines about outbound personal data and 'important data' from China to third countries. Since 1st March 2023, businesses and individuals must comply with these new measures and guidelines or risk penalties. The new guidelines are based on China's data protection and cybers security laws. The purpose of the Measures and the Guidelines is to explain: (i) the circumstances in which security assessments are required for outbound data transfers; and (ii) how such security assessments must be carried out. Since 1st March 2023, data processors must comply with these requirements and must have also addressed any historic non-compliance by this date.

Outbound data transfers include situations in which an entity in China actively sends data to a recipient in another jurisdiction or permits a person or entity outside China to access data generated in the course of the data processor's operations in China. Effectively, the risk does not lie exclusively with entities conducting work in/from China but can also apply to organisations outside of China that access data generated in the course of data processing in China. For multinationals, for example, this would include intragroup transfers of data (e.g. via email and file transfer protocol) and operating centralised document management systems for global operations, with servers hosted outside China.

The new requirement is that data processors must conduct security assessments before engaging in outbound data transfers of data in four circumstances:

- the outbound data transfer involves "important data";
- the outbound data transfer is a transfer of personal information by a critical information infrastructure operator ("CIIO");

- the outbound data transfer is a transfer of personal information by a data processor that has processed personal information relating to 1,000,000 or more data subjects; or
- the outbound data transfer is: (a) a transfer of personal information by a data processor that has made outbound data transfers of personal information relating to 100,000 or more data subjects cumulatively since 1 January of the preceding year; or (b) a transfer of sensitive personal information relating to 10,000 or more data subjects cumulatively since 1 January of the preceding year.

The Chinese privacy legislation, Personal Information Protection Law (PIPL), defines "personal information" as broadly defined as "all kinds of information relating to any identified or identifiable natural person, whether it is in electronic form or any other form, exclusive of any anonymised information". "Important data" is "data that, once tampered with, destroyed, leaked, illegally obtained, or illegally used, may endanger national security, economic operation, social stability, public health and safety, etc.".

The Measures also include a catch-all provision that allows the CAC to specify additional circumstances in which security assessments will be required.

Application Process for Security Assessments

The Measures require data processors to:

1. conduct a self-assessment of their planned outbound data transfers and prepare a self-assessment report.
2. the data processor must then submit the self-assessment (along with certain additional application materials) to the CAC for review.
3. The CAC will then make a decision regarding the transfer.

The factors that the CAC will consider when reviewing application materials include: (i) whether the data processor complies with Chinese laws, administrative regulations, and departmental rules; and (ii) whether the data security protection policies, legislation and cybersecurity environment of the country in which the overseas recipient is located meet the mandatory national standards that apply in China. The self-assessment will further include consideration of the following:

1. The legality, legitimacy, and necessity of the purpose, scope, and methods of data processing by the data controller and foreign recipients;
2. The scale, scope, type, and sensitivity of exported data, and the risks that data export may bring to national security, the public interest, or the lawful rights and interests of individuals or organizations;
3. The responsibilities and obligations undertaken by the foreign recipient, as well as whether the management, technical measures and capabilities to perform the responsibilities and obligations can ensure the security of exported data;
4. The risk that data will be tampered with, destroyed, leaked, lost, transferred, or illegally acquired or used during or after export, and whether channels have been established to safeguard data subjects' rights and interests in their personal information rights;
5. Whether the data security protection responsibilities and obligations have been fully stipulated in the data export-related contracts or other legally effective documents formulated with the foreign recipient; and

Whilst there is no data adequacy agreement between China and the United Kingdom, there are many similarities between the UK GDPR and China's PIPL, the latter framework has brought China's data protection regime more in line with international standards.

If an application is approved, the approval will be valid for two years, but if any key aspects of the security assessment change post-approval, the data processor must reapply.

Data processors should keep their outbound data transfers under review and be prepared to reapply for an assessment if necessary. Should a potential transfer not be approved by the CAC, the data processor may request a reassessment. Any decision made by the CAC regarding a reassessment is final.

Controllers and processors will need to be assessing their planned and existing outbound data transfers and evaluate the compliance obligations they face in light of the Measures and the Guidelines, in order to determine whether they are required to conduct security assessments.

Exemptions

Data handlers in China that are not required, in accordance with Article 40 of the PIPL, to undergo a compulsory security evaluation have three options for legally providing personal information to data recipients outside China in compliance with the existing legal regime [this is if the criteria for outbound transfers does not apply].They may obtain a personal information protection certification, enter into an agreement with the recipients involved in line with the standard contract, or they still undergo a CAC security assessment.

If you are small company or a company that processes small volumes of data in China, it is more suitable to transfer personal information outside of China by entering into a Standard Contract. The Standard Contract provides a suitable way for overseas entities to transfer personal information outside of China.

Standard Contract for Cross-Border Transfers of Personal Information

Under the PIPL, before transferring personal information ("PI") out of China, PI handlers currently must satisfy one of the following procedural requirements:

- Pass a security assessment ("Security Assessment") by the CAC;
- Obtain a PI protection certification from a CAC authorized institution; or
- Enter into a Standard Contract ("SC") with the data recipient.

The Measures require:

- The parties to use the template Standard Contract attached to the Measures. The parties may add provisions as long as they do not conflict with the Standard Contract;
- The Personal Information handler to file the SC with the provincial level CAC within 10 business days after the Standard Contract becomes effective, together with the related Personal Information risk assessment; and
- Recipients outside of China to notify the Personal Information handler immediately if they receive a request from a foreign government to provide PI transferred under the Standard Contract.

China Issued Draft Personal Information Audit Measures

According to the Draft Audit Measures, any personal information processor in China should conduct the compliance audit on its personal information processing activities.

Different from the General Data Protection Regulation ("**GDPR**") of EU, there is no such a conceptual difference between "processor" and "controller" under Chinese law. Both of them are "personal information processors" under Chinese law, i.e., any entity that collects, stores, shares, transfers or otherwise processes personal information will be deemed a personal information processor, even if it processes personal information upon other's instructions.

A personal information processor that fails to conduct the compliance

audit may be subject to administrative penalties under the Personal Information Protection Law of China ("**PIPL**") or even criminal liabilities if it constitutes a criminal offense.

A personal information processor that fails to conduct the compliance audit may be subject to administrative penalties under the Personal Information Protection Law of China ("**PIPL**") or even criminal liabilities if it constitutes a criminal offense.

Further information:
https://www.jonesday.com/en/insights/2023/03/china-finalizes-measures-on-the-standard-contract-for-crossborder-transfers-of-personal-information

https://www.dentons.com/en/insights/articles/2023/march/2/new-measures-on-standard-contract-for-cross-border-transfer-of-personal-information

https://www.zhonglun.com/Content/2023/08-09/1422169733.html

Takeaways

The key takeaways are as follows:

1. Businesses should assess their planned and existing outbound data transfers and evaluate the compliance obligations they face in light of the Measures and the Guidelines, in order to determine whether they are required to conduct security assessments.
2. Businesses should identify and address any instances of non-compliance.
3. Businesses should take concrete steps to ensure that compliance and IT functions have the necessary staff, resources, and mandate to conduct self-assessments and take remedial actions as appropriate.
4. Businesses should evaluate their data privacy policies and practices and conduct self-assessments promptly, to leave sufficient time for remediation and adjustments.
5. Businesses should keep an eye out for further implementing regulations or industry-specific guidance related to the Measures and the Guidelines.

Q&A

Regarding collecting data responses in China. We host the survey data collected but access responses via a panel provider. Is this permissible under the new regulations? Not clear if the risk and responsibility lies only with a China based firm sending data to our UK firm?

This is permissible under the new regulations; however, we advise that you liaise with your providers/processors based in China. Dependent on the size of outbound data, they may be required to undertake these measures. Outbound data transfers include situations in which an entity in China actively sends data to a recipient in another jurisdiction or permits a person or entity outside China to access data generated in the course of the data processor's operations in China

Could we please have any further information available on data collection from *China* and how this might impact on data being shared with us from our partners there and how the information must be stored.

Please see above. If you have partners based in China, we advise liaising with them.

What the implications are for market research companies who might do some research with Chinese respondents?

As outlined above, you must identify if you meet the criteria to fulfil the new obligations, if so, you must undertake the relevant assessments. If not, you can continue with undertaking Standard Contracts, see 'Exemptions'.

Resources

https://www.dentons.com/en/insights/articles/2022/october/11/outbound-data-transfers-of-personal-information-in-china

https://www.whitecase.com/insight-alert/new-requirements-outbound-data-transfers-china#:~:text=4%20Article%2019%20of%20the,and%20safety%2C%20etc.%22.

https://focus.cbbc.org/what-do-chinas-data-protection-laws-mean-for-uk-higher-education/

https://hsfnotes.com/data/2023/03/06/china-officially-releases-standard-contract-for-cross-border-transfer-of-personal-data/