

Data Compliance Update

R&P News

Page 2

**Deadline for Security Assessment
of Outbound Data Transfer**

Page 3

**New Rules for Small-Scale
Exporters of Personal Information**

Page 4

**China Data Compliance through
Protection Impact Assessment
(PIA)**

Page 5

**China Data Compliance Action
Lists**

Page 6

**R&P RECOGNIZED IN
2023 BY:**

Chambers
AND PARTNERS



In this Legal Briefing, we focus on **data privacy compliance**. China is quickly establishing a comprehensive system for securing personal information, with some similarities to GDPR but with Chinese characteristics. This is relevant to many companies, including:

1. Companies with subsidiaries in China and companies based outside of China that **collect large amounts of personal information within China and transfer these outbound**, as they need to complete a security assessment filing with the CAC; the original deadline was 28 February 2023 (p. 3).
2. Companies that **export personal information on a small scale**, as they should still complete an impact self-assessment (PIA) (p. 6); and sign the Standard Contractual Clauses (SCC) with the overseas recipients. Filings are due by 30 November 2023 (p. 5).

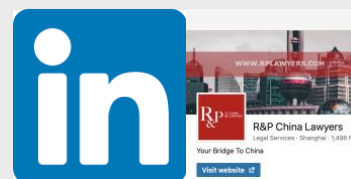
For an introduction to the new implementing regulations for data and what they do mean for your company, find our detailed article on our [website](#) or reach out to us.

We trust these articles will help you understand the latest on a complex and evolving topic, and enable you to make decisions on how to be and remain data-compliant in China!

Stay connected with us for regular updates via:

LinkedIn

Click the link to get to our [Company Page on LinkedIn](#) and Follow us together with some 3,000 contacts!



R&P NEWS

R&P Welcomes New Partners Limeng Yang and Eric Yuan

We are pleased to announce that two of our colleagues have been appointed as Partner.

Ms. [Limeng Yang](#) focuses on complex dispute resolution, representing clients in litigation & arbitration all over China.

Mr. [Eric Yuan](#) heads R&P's employment practice, and specializes in redundancy projects and senior management terminations.

Read the full news item [here](#).

Senior Data Protection Lawyer Connie Chen joins R&P

R&P is very pleased to announce that Ms. [Connie Chen](#) has joined our team. Connie has a strong background in the retail industry, providing legal support to international brands in China. In recent years she has pivoted towards data privacy and cyber-security, supporting multinational clients on building compliance systems, performing data assessments, and completing filings with the Cyberspace Administration of China (CAC).

Read the full news item [here](#).



Deadlines for Security Assessment of Outbound Data Transfer

By Connie Chen and Maarten Roos

Our article outlines the security assessment process for companies in China and abroad that transfer large amounts of personal information outside of China, as required under the PRC Personal Information Protection Law (PIPL).

Passing the security assessment of the Cybersecurity Administration of China (CAC) is a prerequisite to compliantly transferring large volumes of personal information from China to recipients overseas. Companies that fall within this scope include both entities in China and foreign companies collecting data in China, as long as certain thresholds are met.

The deadline for completing the assessment was 28 February 2023, and failure to complete the assessment can have major repercussions for businesses. The assessment process is complicated and time-consuming, and involves an internal assessment and application material preparation, and then the CAC's approval process.

Key steps are the full mapping of internal data assets, organizing and assessing data security

management systems and technical measures, checking with overseas data recipients on their processes, and conducting due diligence on the legal and cyber security environment of the recipient's jurisdiction.

Given the complexity of the assessment process, many companies are still in the process of completing these steps. The recommendation is for companies to start the process as soon as possible and to make progress towards the final goal of completing a full security assessment. While the CAC is expected to initially be lenient, it is important for companies to take this deadline seriously and to take immediate steps to comply with the law.

Find our full article on the security assessment on our [website](#).



New Rules for Small-Scale Exporters of Personal Information

By Maarten Roos and Connie Chen

China's Cyberspace Administration (CAC) has introduced new measures and Standard Contractual Clauses (SCC) to regulate cross-border transfer of personal data under China's Personal Information Protection Law (PIPL) by small-scale data exporters.

The Measures apply to companies that export personal information overseas, but do not meet the criteria and thresholds that subject them to the CAC's data security assessment and prefer to avoid a certification process with a CAC-appointed body.

In practice, most subsidiaries of international companies are expected to fall into this category.

Such exporters are required to sign SCCs with overseas recipients and complete a personal information protection impact self-assessment (PIA) and file both with the CAC.

The Measures establish a six-month grace period for existing exporters to file, and include specific requirements for the PIA, which we outline in our next article.

Overall, the introduction of new measures and SCCs is a major step towards the establishment of a comprehensive legal regime in China for the protection of personal information, emphasizing the importance of compliance for companies involved in cross-border transfer of personal data.

Find our full article on the security assessment on our [website](#)

Stay connected with us for regular updates via:

WeChat

Scan our WeChat QR code and follow our updates.





China Data Compliance through Protection Impact Assessment (PIA)

By Sylvia Wang and Connie Chen

With China's increasing focus on protecting personal data, regulatory agencies are taking a closer look at the treatment of personal data, and enforcement of relevant laws should be taken into account for regular business activities. Therefore businesses need to review in how far they meet the Chinese legal standards for personal data compliance.

A Protection Impact Assessment (PIA) is a self-examination by a company on the personal information's full lifecycle, including collection, storage, use, processing, transmission, disclosure, and deletion. Companies should conduct impact assessments not only to fulfill their privacy protection responsibility under laws and regulations but also to prepare a defense for itself in the event of a data security incident.

PIAs are fast becoming a cornerstone of strategies to comply with Chinese data compliance regulations. In practice, companies generally need to first distinguish different business scenarios and then complete an in-depth analysis. Extensive information is generally collected for a PIA, such as the type and amount of data to be processed, processing purpose and legal basis, key processing activities, impact on information subjects' rights, measures taken, and data security incidents in the past.

Three dimensions and several departments are involved during the PIA. The legal department, or an external law firm with experience in this area, usually takes the lead in conducting the PIA. The IT department is involved to review and analyze whether the company's data security protection measures are effective, and the HR department is involved to review the internal rules and regulations of the enterprise. All of the above will be integrated into an impact assessment report.

The PIA is a good starting point for companies to better understand China's rules on data protection and how far the company is in compliance with those rules. However, a PIA is only the first step in an ongoing effort to improve compliance in this area. Companies will need to take continuous measures to comply with the developing regulatory requirements, and in practice, the results of one impact assessment will usually serve as reference to the next one.

Find our full article on PIAs on our [website](#).

China Outbound Data Compliance Action List

To help ensure that your company is in compliance with these regulations, consider following the China Outbound Data Compliance Action List outlined below.

1. Determine if Your Company is Required to Complete a Government Security Assessment for Outbound Data Transfer

Conduct a data mapping on your company's data pool, look into the personal data scale and data importancy you are exporting, then determine whether the data you process reaches the threshold of a government-led security assessment for outbound data transfer. If yes, take immediate action to ensure that the necessary assessment are completed timely as it is already overdue. You may review the detailed information provided in the [Deadline for Security Assessment for Outbound Data Transfer](#) article.

2. Fulfill requirements for Small-Scale Personal Data Exporters in China

If your company is a small-scale exporter of personal data, you are NOT subject to the government-led security assessment, however, you are still required to be compliance with other requirements, such as entering into standard contract with data importer. You may review the new rules and requirements for small-scale personal data exporters in China, as outlined in the [New Rules in China for Small-Scale Personal Data Exporters](#) article.

3. Complete Personal Data Protection Impact Assessments Requirements

In either case - to apply for a government security assessment, or to fulfil requirements of a small-scale data exporter, a personal data protection impact self-assessments (PIA) is required. You may review the guidelines outlined in the [China Data Compliance through Personal Data Protection Impact Assessment](#) article for further information.

On-going China Data Compliance Action List

The PIA is also a good starting point for your companies to better understand China's rules on data protection, and a practical guidance for you to take appropriate measures to comply with continuously developing regulatory requirements. Here are some examples of measures you may consider to deploy for personal data compliance:

1. Update Your Company's Data Protection Policies and Procedures

To ensure compliance with the regulations, review and update your company's data protection policies and procedures to ensure that they are in line with the requirements.

2. Train Employees and Contractors on the New Data Compliance Regulations

To ensure that all employees and contractors understand the data compliance regulations and their responsibilities to comply with these regulations, conduct training sessions on a regular basis.

3. Conduct Regular Audits and Consider Hiring a Third-Party Auditor

To ensure ongoing compliance with the regulations, conduct regular audits to ensure that your company's data processing practices remain in compliance with the regulations. Consider hiring a third-party auditor to conduct an independent review of your company's data processing practices for compliance with the new regulations.