China Personal Information Protection Impact Assessment (PIPIA) Template Version 1.0

Export of data from People's Republic of China > *INSERT COUNTRY*

Important Note: *This template is an example of how you can record your impact assessment and outcomes. It follows the limited guidance set out by the Cyberspace Administration of China and is subject to change pending further guidelines. It should be read alongside that guidance, China's Standard Contractual Clauses and the PIPL, and in concert with appropriate legal counsel.*

Document Control	
Date of assessment	
Author	
Reviewed by	
Review Date	

Decision Summary	
Importer Details	
Third Country Details	

Purpose of Transfer	
Can the Transfer Take Place?	
Decision Approved by:	

Glossary of Terms	
Exporter	Data exporter is a processor established in the People's Republic of China (PRC) that transfers personal data to a data importer outside of the PRC.
Importer	Data importer is a controller or processor established outside the PRC that receives personal data from a data exporter inside the PRC.
Processor	Article 73 of the PIPL defines a personal information processor as 'any organisation or individual that independently determines the purpose and method of processing in personal information processing activities.' Note that this maps to the term 'controller' in other privacy laws, such as GDPR.
Sensitive Data	Sensitive Personal Information is defined in Article 28 of the PIPL and refers to 'personal information that can easily lead to the infringement of the personal dignity or natural persons or the harm of personal or property safety once leaked or illegally used, including such information as biometrics, religious belief, specific identities, medical health, financial accounts, and whereabouts, and the personal information of minors under the age of 14.'
Public Authorities	Public Authority means any government or other public administration, including public advisory bodies, at national, regional or local level or any natural or legal person

	performing public administrative functions under national law.
Legal Basis	Article 13 of the PIPL provides that 'Only under any of the following circumstances may a personal information processor process personal information: (I) where the consent of the individual concerned is obtained; (II) where it is necessary for the conclusion or performance of a contract to which the individual concerned is a party, or to implement human resources management in accordance with labour rules and regulations formulated according to law and collective contracts concluded according to law; (III) where it is necessary for the performance of statutory duties or statutory obligations; (IV) where it is necessary for coping with public health emergencies or for the protection of the life, health, and property safety of a natural person; (V) where such acts as news reporting and supervision by public opinions are carried out for the public interest, and the processing of personal information is within a reasonable scope; (VI) where the personal information disclosed by individuals themselves or other legally disclosed personal information is processed within a reasonable scope in accordance with the provisions of this Law; and (VII) other circumstances provided by laws and administrative regulations. Individual consent shall be obtained for the processing of personal information stipulated in the other clauses of this Law, but in the circumstances specified in the preceding paragraph from (II) to (VII), the individual's consent is not required.

References	
Personal Information Protection Law of the People's Republic of China (PIPL)	English (Official)
PRC Standard Contractual Clauses	English (Unofficial)
Data Security Law of the People's Republic of China	English (Official)
Security Assessment Measures	English (Unofficial)

Notes on Completing the PIPIA

Some important points to consider when completing the PIPIA:

1. This PIPIA template assumes you have a good understanding of your international transfers outside of the PRC already. If you do not know what international transfers your organisation is engaged in then you should first map your transfers.

2. This PIPIA can be used to assess international transfers of personal data from the PRC to organisations outside the PRC, including via onward transfers to additional foreign recipients.

3. It is ultimately the responsibility of the exporter to complete the PIPIA. However the importer is likely to have a better understanding of the local legal regime in the destination country and so it may be easier to have the importer complete or assist with completion of certain sections of the PIPIA.

4. The PIPIA contains guidance notes throughout to help you complete the assessment. These are in *blue highlights* - please delete from your final PIPIA!

5. Don't forget the other PIPL requirements for the processing! A PIPIA in this context is just one assessment that relates specifically to the international transfer of data outside of the PRC. The processing in general still needs to be in compliance with PIPL.

6. The PIPIA sits alongside and complements the PRC China Standard Contractual Clauses, which must also be executed between the parties.

7. This PIPIA is intended to fulfil obligations only when relying on the PRC Standard Contractual Clauses as a data export mechanism. **This self assessment is not intended to be used to facilitate the other export measures:**

    a. (Undergo a mandatory CAC-administered security assessment (CAC Security Assessment);
    b. Obtain a personal information protection certification from a CAC-recognized professional institution (Security Certification);

8. A Processor must file (i) the executed Standard Contract and (ii) the PIPIA report to the provincial level counterpart of CAC within 10 working days after the Standard Contract comes into effect.

Details of the importer and exporter	
Name of the Data Exporter	
Name of the Data Importer	
Is the importer a private organisation or a government authority/body?	
The scale, scope, type and degree of sensitivity of the personal information exported *This section should be used to detail the particular circumstances and contexts of the transfer, and the details recorded here should be considered when assessing the risks the transfer might pose to the rights and freedoms of the data subjects that will be conducted later in the PIPIA.*	
Which country is data being transferred to?	*For data transfers to an importer based in multiple jurisdictions, a separate analysis should be completed for each country that data is transferred to. .*
What is the purpose of the processing activity for which data is transferred?	
Will the transfer be systematic or on an as-needed/ad hoc/one off basis?	
Number of individual's data exported?	
Categories of data subject	*ie customer, client, patient, employee etc*
Categories of personal data transferred	*ie name, address, ID number etc*
Is Sensitive Data transferred?	

Is data relating to children transferred?	
Will data be stored by the importer or will the importer only access data via remote access to data stored in China?	
The legality, legitimacy and necessity of the processing and data subject rights	
What is the legal basis for processing?	*See the Glossary of Terms for the PIPL Legal Bases.*
Is the export of data necessary to achieve the purpose of the processing? Can the purpose be achieved without the export of data?	
What channels are available to data subjects to exercise their rights and interests in their personal information?	
The obligations to be undertaken by the foreign recipient and its capability	
Describe the technical measures to be adopted by the foreign recipient to protect the personal information received:	
Describe the organisational measures to be adopted by the foreign recipient to protect the personal information received;	
Does the recipient have the capacity to perform its obligations to ensure the security of the processing?	

The impact of the personal information protection laws, regulations and policies of the foreign recipient's jurisdiction on the performance of the SCCs.

This section prompts you to assess the legal regime in the third country, in general terms and related to privacy law specifically.

We essentially need to assess whether the Standard Contractual Clause can be enforced, if necessary, in the third country, by either the exporter or the data subjects.

This means that we should consider whether both exporter and data subject have access to enforceable and effective legal remedies in the third country. For example, if the third country has no effective rule of law then it is difficult to envisage a data subject being able to bring effective action against the importer to enforce their rights.

We also need to assess whether the third country offers safeguards and protections that govern public authority access to personal data.

Note that in the case of transfers to multiple third countries, the following section should be completed for each jurisdiction.

Number of historic requests for access to data by government authorities?	
Describe the rule of law in the third country, in general terms	*This can be a high level overview. You should be able to draw on NGO reports, government papers and media articles to develop an understanding of the state of the rule of law in the third country.* *Some important factors to consider:* ● *Independence of the judiciary* ● *Independence of judicial process* ● *Access to justice via court systems* *Cite references to back up your assessment.* *You do not need to be exhaustive!*
Describe the country's approach to human rights	*Again, this can be a high level overview. You should be able to draw on NGO reports, government papers and media articles to develop an understanding of the state of human rights in the third country.* *Cite references to back up your assessment.*

	You do not need to be exhaustive!
Are foreign judgments or arbitration awards recognised or fairly enforced?	*One way to determine this is to assess whether the third country is party to conventions for recognition of enforcement of foreign judgments or arbitration awards (such as the Brussels Convention/ the Hague Choice of Court Convention).*
Does the country have a privacy law? If so, describe.	*Describe the privacy law in the third country. You may wish to consider the following aspects of the law:* • *Does the privacy law have foundational principles?* • *Does the law contain lawful bases under which data must be processed?* • *Does the law have data minimization requirements?* • *Does the law mandate personal data accuracy?* • *Does the law require that data is processed securely?* • *Does the law grant individuals with rights and freedoms concerning use of their personal data?* • *Does the law contain provisions for the processing of sensitive data types?* • *Does the law contain obligations relating to automated decision making and profiling?* • *Is there an independent and effective supervisory authority?* • *Does the supervisory authority have tools (enforcement action) to encourage compliance?*
What laws govern the state/public authority access to personal data?	*List the surveillance laws which apply to the Data Importer based on which public authorities may request access to the personal data*
Is this legal framework based on the rule of law and governed by clear, proportionate and necessary legal rules?	*You should be able to draw on NGO reports, government papers and media articles to develop an understanding of the public authority's access to data.*
Do individuals have fair redress to data processed by public authorities?	
Does an independent and impartial oversight system exist to oversee public authorities' access to personal data?	

Do public authorities publish transparency information about surveillance and data access?	
How is data sharing between public authorities governed?	
Is the data importer legally entitled to challenge/object to requests for access to personal data from public authorities?	
Summary Decisions and Risk Assessment	
Are Standard Contractual Clauses enforceable in the third country?	*Using the information recorded above in the PIPL, come to a balanced and reasonable assessment on whether you believe that the SCC will be enforceable in the third country legal system.*
How likely is public authority access to the transferred data?	*Assess the likelihood of access to data, given the context of the transfer:* *Remote* *Low* *Moderate* *High* *It is important to give as detailed a rationale as possible here in determining the risk rating.* *You should specifically consider:* - *The details of the applicable laws that facilitate government access to data and the types of data that the authorities are typically concerned with.* - *Whether the importer has ever received such requests and the frequency of such requests.* - *Whether there is evidence that other companies or organisations in similar industries have received such requests.* - *You can draw on case law, transparency reports and other statutory/regulatory publications as appropriate.*

Describe the potential risks to the rights and interests of the data subjects	*Briefly describe the risks to the data subjects relating to the processing as a whole. This should be similar conceptually to the risk assessments conducted in a PIA/DPIA.* *The risks here can relate to the processing in general, not just specifically to the data export.*
Describe the potential risks of personal information being altered, destroyed, leaked, lost, or further transferred, or illegally used;	*Briefly describe the risk of data breach.*
Overall Risk Level	*Use your local risk assessment methodology to assign an overall risk level to the processing, including the data export.*
Comments and Recommendations	*Use this section to make recommendations about whether the export can go ahead, and whether any further measures need to be in place to mitigate any risks.*