International Transfer of Research Data

Updated 5 February 2025

In Brief

When Curtin University researchers are gathering personal data from overseas jurisdictions, they must determine the data protection and privacy laws that exist and how those laws apply both where the data is being gathered as well as in Australia. These laws may restrict how personal information is collected, processed, stored, and shared.

Below are some FAQs regarding the current data protection and privacy laws of China (Personal Information Protection Law) and the European Union (EU) (General Data Protection Regulation) as examples of two regions with similar laws that each seek to address these issues. These FAQs have been prepared by the Foreign Risk Management and Library Research Services Teams and are not exhaustive, however, provide a broad overview of how these laws may affect research. They are intended as a guide to help researchers consider the appropriate structure and scope of research and research data plans as required. Other countries with similar data protection laws include, but are not limited to, Brazil, India, Japan, South Korea and the UK.

The information presented should not be taken as legal advice.

It is the researcher's responsibility to determine what laws are applicable to their research project and what measures they will need to take to ensure compliance with Australian legislation and laws where the data is being collected, including consent requirements, notices, impact assessments and representative nominations where required.

Personal Information Protection Law (PIPL) - China

Researchers may find a translation of the PIPL legal text useful.

What data is regulated under China's PIPL?

Academic/research data is exempt from regulation except for the following scenarios:

- more than 100,000 individuals
- data that contains **personal information (inc. sensitive personal information)** or **important data.**

What is 'personal information'?

Personal information is any type of information that identifies or can identify a person. It does not include anonymized information.

Handling of personal information includes the collection, storage, use, processing, transmission, provision, disclosure, deletion etc., of personal information. (PIPL, Article 4)

What is 'sensitive personal information'?

Sensitive personal information is information that if leaked or illegally used can cause harm to the subjects' dignity or property.

Examples include:

- biometric identifiers
- religious faith
- any particular identities
- medical care and health
- financial status
- location tracking
- any personal information of minors under the age of 14. (PIPL, Article 28)

What is 'important data'?

Important data is understood to be *"data specific to certain fields, groups, and regions, or reaching a certain level of precision and scale that, once leaked, tampered with, or destroyed, may directly jeopardize national security, economic operation, social stability, public health, and safety."* (Cybersecurity Law of PRC & Data Security Law)

Definitions provided by various legislative instruments are not entirely consistent, however, they all reflect the above principles. Ultimately, the scope of important data will be determined by a variety of regulatory officials in China, each of whom will have substantial discretion to define what should be considered important data and how this data should be handled. It is recommended to take appropriate risk mitigation measures if you believe you will be handling important data.

Data which has a geostrategic relevance (e.g. relating to rare earth elements), has a clear applicable dual military or security use, or which Curtin considers 'sensitive' (and specifically relates to China) are examples which may be considered important data.

Research containing 'Personal Information' or 'Important Data'

Does China's PIPL require providing a privacy notice when handling personal information or important data?

Yes, all data subjects must be provided with a privacy notice which informs them of:

- The organisational or personal name of the personal information handlers.
- The purpose and method of collecting the subject's personal data, the type of personal information handled, and the period it will be stored.
- Their rights to inquire, access, edit, delete, restrict or refuse, withdraw consent, etc.
- The transfer of data subjects' personal data to Cloud Service Providers, third parties processing the data on behalf of the organisation, or recipient outside the country. (PIPL, Article 17)

Does China's PIPL require obtaining data subject consent?

Subject's consent must be given voluntarily and explicitly by individuals who are fully informed. Where there are changes to the purpose or methods of handling information, or the type of personal information to be handled, the individual's consent shall be newly obtained. (PIPL, Article 14)

Individuals have the rights to know about, decide on, limit use of, or withdraw their consent at any time. The personal information handler must provide a convenient and easy method for withdrawing consent.

The PIPL also grants individuals the right to access and copy their personal information, as well as correct or supplement their personal information if incorrect or incomplete. (PIPL, Article 45-46)

Will I require a data protection impact assessment or other category of risk assessment?

Under Article 55 of the PIPL, a personal information handler *must* conduct a Personal Information Protection Impact Assessment (PIPIA) if they:

- **Handle sensitive personal information**
- Entrusts personal information handling, provides personal information to other personal information handlers, or discloses personal information
- Provides personal information abroad
- Engages in other personal information handling activities that have a 'major influence' on individuals

The PIPIA must assess:

- The legality, legitimacy and necessity of the purpose, scope and processing method of the data processor [in China] and the overseas recipient.
- The scale, type, sensitivity, and risks of exporting personal information, and its potential impact on the subjects' rights and interests.
- The responsibilities and obligations of the overseas recipient, including the management and technical measures taken to secure exported personal information.
- The risk of the personal information being tampered with, destroyed, leaked, lost, or misused, and whether the channels for protecting the rights and interests of the subjects are unobstructed.

- The impact of the overseas recipient's local data protection policies and regulations on fulfilling date protection obligations.
- Other matters that may affect the security of the outbound personal information.

These reports must be preserved for at least three years.

A template for the PIPIA is included below.

Am I required to appoint a representative in China?

If you are handling personal information of people in China while overseas, you are required to appoint a designated representative within China. You must disclose the name, contact information, and other information in your PIPIA. (PIPL, Article 53)

What are the penalties for violating the PIPL?

Failure to comply with this legislation can result in warnings, confiscation of data, termination of improper practices, fines of up to $20,000 AUD against individuals and fines of up to $10 million AUD against institutions.

PIPIA template

1. Project Overview

- Project Name:
- Responsible Department/Researcher:
- Date of Assessment:
- Purpose of Data Processing:
- Scope of Personal Information:
  (e.g., types of data collected, data subjects involved)

2. Description of Processing Activities

- Nature of processing:
  (e.g., collection, storage, use, transfer, deletion)
- Method of Processing:
  (e.g., manual input, automated systems)
- Location:
  (e.g., domestic, cross-border transfers)

3. Assessment of Legal Basis

- Purpose and Necessity:
  (Explain why the data processing is necessary and lawful.)
- Compliance with PIPL Principles:
  - legality
  - transparency
  - necessity
  - proportionality

4. Risk Analysis

- Risks to Individuals:
  - Potential for data tampering, destruction, leakage, loss, or illegal use.
  - Impact on the rights and interests of data subjects.
- Nature of Data:
  (Identify whether sensitive personal information is involved.)
- Cross-border Risks:
  (Assess the impact of transferring data internationally and compliance with overseas legal frameworks.)

5. Security Measures

- Technical Measures:
  (e.g., encryption, access controls, data anonymization)
- Organizational Measures:
  (e.g., training, internal audits, access policies)
- Emergency Plans:
  (e.g., incident response protocols for breaches)

6. Mitigation Strategies

- Recommendations for Risk Mitigation:
  - Steps to reduce high risks identified in the assessment.
  - Any additional technical, organizational, or legal safeguards.

7. Review of Overseas Data Transfers (if applicable)

- Recipient Information:
  (Country/region, recipient details)
- Impact of Local Regulations:
  (How the destination country's laws may affect data protection.)
- Contractual Safeguards:
  (e.g., standard contracts as required by PIPL.)

General Data Protection Regulation (GDPR) - EU

Researchers may find the GDPR legal text useful.

What is the GDPR?

The General Data Protection Regulation (GDPR) aims to give individuals control over how their personal data is used, maintained, and shared.

The GDPR applies to all individuals residing in or who are citizens of the European Union (EU) or the European Economic Area (EEA). The GDPR includes citizens of these groups who currently live outside Europe.

What countries make up the GDPR?

Austria, Belgium, Bulgaria, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, The Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

What is 'personal data'?

Personal data is defined as any information about a person that can identify them, either directly or indirectly. Examples of personal data include a person's name, e-mail address, government issued identifier, or other unique identifier such as an IP address or cookie number, and personal characteristics, including photographs.

There is a category referred to as **sensitive personal data** which merits a higher level of protection. Special categories of personal data include several items that are often collected as part of a research study, including information about a data subject's:

- health
- genetics
- race or ethnic origin
- biometrics for identification purposes
- sex life or sexual orientation
- political opinions, religious or philosophical beliefs
- trade union membership.

Criminal convictions and records, while not among the "special categories" of personal data, also receive heightened protection under the GDPR.

It is not necessary to have a name associated with the information. If the information, taken in the aggregate, could be used to identify a person, it is personal data protected by the GDPR.

Is anonymised data regulated under the GDPR?

No, if a data set is anonymised the GDPR does not apply. The anonymisation process can occur at the point of collection or anonymised post-collection. For the data to be truly "anonymised" under GDPR, it must be irreversibly altered such that it is impossible to re-identify an individual, even with access to additional data. If there remains a possibility of re-identification, even if it's remote, the data is still considered pseudonymised rather than anonymous and remains subject to GDPR regulations. It is recommended, where possible, to anonymise research data.

Does the GDPR require a privacy notice?

Yes, all data subjects must be provided with a privacy notice which clearly explains:

- The identity and contact details of the data controller.
- The purpose and legal basis for processing the data.
- Who will receive the data.
- How long the data will be kept.
- Individuals' rights over their data (e.g. access, correction, deletion).
- If data will be transferred outside the EU.
- The rights to lodge a complaint with a data authority.
- If automated-decision making is involved.

The notice should be given before or at the time of data collection and must be clear and easy to understand.

Does the GDPR require obtaining data subject consent?

Yes, consent must be obtained when processing personal data. For consent to be valid under the GDPR, individuals must give clear, informed and voluntary consent for their data to be processed. Consent must always be easy to withdraw, and individuals should be fully informed about how their data will be used.

Research subjects can obtain copies of all their personal data and have the right to withdraw consent at any time. Upon withdrawal, researchers can no longer retain the personal data for the purpose of research, including in pseudonymised form.

Will I require a Data Protection Impact Assessment (DPIA)?

A DPIA is required if you are processing sensitive personal data. The DPIA should outline specific information to assess and mitigate the risks associated with the processing of personal data, and include:

- *Description of the Processing:* Details of the data processing activities, including the purpose, scope, and methods used.
- *Necessity and Proportionality:* Justification for the processing, ensuring data minimization and relevance.
- *Risk Assessment:* Analysis of potential risks to individuals' privacy and data security
- *Mitigation Measures:* Steps to reduce or manage the identified risks, such as encryption or access controls.
- *Consultation with the Data Protection Authority (DPA):* If high risks remain, the relevant Data Protection Authority must be consulted. Each member state has a responsible DPA.
- *Data Subject Protection:* How individuals' rights and interests will be safeguarded
- *Ongoing Review:* Plans for regular monitoring and evaluation of the processing and mitigation measures.

Researchers may find the template provided by the Information Commissioner's Office UK (ICO) for DPIAs a useful example.

Am I required to appoint a representative in Europe?

Yes, if you are based outside of the EU/EAA but process personal data of individuals within the EU/EEA you must appoint a representative within the EU/EEA.

How is the GDPR enforced?

Individual data protection authorities (DPAs) from the 27 EU member states enforce the GDPR. DPAs are independent public authorities who investigate complaints, provide advice on data protection issues and determine when the GDPR has been breached.

What are the potential penalties?

Failure to comply with this legislation can result in:

- warnings
- temporary or definitive bans on processing personal data
- lower-tier fines of up to €10 million for breaches such as inadequate record-keeping or failing to notify authorities of data breaches
- higher-tier fines of up to €20 million for serious breaches such as failure to obtain consent, violating data subject rights, or unlawfully transferring data outside the EU.