TrustArc

China's PIPL

Frequently Asked Questions

Last Updated: 21 September 2021

This paper provides commonly asked questions on the People's Republic of China's new Personal Information Protection Law (PIPL). It will be updated with new information as such information is received or clarified. As always, keep in mind that this is guidance based on our expertise in global privacy laws, but is not legal advice.

We will continue to update these FAQs with new questions. If there is a significant clarification on some of the items that are not clear at this time, we will post a blog or otherwise communicate the clarifications outside these FAQs.

Key Definitions & Scope

1. When does PIPL apply?

PIPL applies to all personal information handled (*processed*) within the territory of the People's Republic of China. In addition, it applies when products or services are offered to natural persons in China, or when their activities are assessed or analyzed. Laws and administrative regulations can further extend the scope of PIPL.

PIPL does not require a nationality requirement and therefore does not apply to all people with a Chinese passport, wherever they are located. Like the General Data Protection Regulation (GDPR) out of the European Union (EU), PIPL applies on the basis of the location of the individual as well as on where the data processing takes place. This also means that PIPL applies to anyone within the borders of China, no matter their nationality or habitual place of residency.

At this time, there is no further information on what is considered as "offering products or services to natural persons in China." However, it is unlikely an occasional purchase from China on a non-Chinese website with no indicators that it is designed to be available in China (e.g., not available in a Chinese language, no payment in Chinese currency), would be covered by PIPL. The reverse would also be true: having a website in a Chinese language, with the option to pay in a Chinese currency and/or shipment to China, would likely fall within the scope of PIPL.

2. Is PIPL applicable to organizations whose vendors handle personal data of China residents, however, the data is hosted outside of China?

In general: yes, as long as the condition is met that products or services are offered to natural persons in China. The hosting of the data outside China will also need to comply with the cross-border transfer requirements.

3. If an entity lawfully obtains personal information that is subsequently anonymized, can the entity use that data for any further purpose of its choosing, regardless of the initial basis of collection?

Yes, if the data are truly anonymized. This means that it should be impossible to distinguish specific natural persons as well as impossible to restore the data to their original state.

4. Does PIPL contain exceptions for business to business (B2B) relations?

No, the law does not specifically exclude personal information handled in a B2B context. However, if a particular law outside PIPL applies to your activities and B2B is exempt, China includes a variety of references to following other laws as indicated. This is something you need to determine outside these FAQs.

This debate that offering products or services to natural persons incorporates B2B is the same as the one under the General Data Protection Regulation Article 3(2). There is no clear answer. The European Union authorities have not spoken to it and at this time, the Chinese authorities have not clarified.

5. Does PIPL contain exceptions for small and medium size enterprises?

No, the law does not contain such exceptions or exemptions.

6. Does PIPL contain a data residency requirement?

Yes, government agencies must store their data within China as well as organizations who are processing data for the purposes of fulfilling their statutory duties. Otherwise, there is no explicit requirement, but there are strict requirements for transferring data outside China.

7. What is considered a critical information infrastructure operator or entity, processing a large amount of personal information?

As determined in Art. 40 PIPL, these definitions will be provided by the Cyberspace Administration of China (CAC). A specific timeline is not yet known.

8. How would PIPL apply to data held in the cloud?

Handling personal information in the cloud is fully covered by PIPL and therefore subject to all requirements of the law. Please note that cloud processing might be subject to cross-border transfer rules if the data is hosted outside China and or accessed from another jurisdiction.

9. Does PIPL apply in Hong Kong, Macau, and Taiwan?

Hong Kong and Macau both have the status as Special Administrative Regions within the People's Republic of China, allowing them to adopt their own legislation on a range of topics. Both regions have done so for data protection, with the Hong Kong Personal Data (Privacy) Ordinance and the Macau Personal Data Protection Act respectively. At this time, there are no indications PIPL will overrule these pre-existing data protection laws. The Macao Data Protection Authority has issued a statement calling on local data handlers to comply with PIPL, given the likelihood that data handling in Macao would include personal information covered by the Chinese law.

As to Taiwan, the situation is less clear, given that the status of the island is disputed. The Republic of China has adopted its own Personal Data Protection Act for Taiwan, which has most recently been amended in 2015. However, the government of the People's Republic of China considers Taiwan to be one of their provinces, which would imply application of PIPL. TrustArc is not in a position to determine which of these laws should prevail.

10. Does PIPL apply to Chinese students who apply to a higher education institution from China, but then attend outside of China?

It is likely the initial collection of personal information, e.g. during the application phase, would be covered by PIPL, since this would be data handling following the offering of (education) services to prospective students in China. Once the student arrives at the institution, they would be subject to the local data protection legislation only.

11. Is there more information on what is understood by "specific identity" or "specially-designated status" in Art. 28 PIPL [terminology varies depending on the translation used]?

At this time, there is not.

12. What is the impact of the inclusion of financial data as sensitive data?

This means that the possibilities to process financial information are restricted and need to meet the requirements of Art. 28 et seq.: "Only where there is a specific purpose and a need to fulfill, and under circumstances of strict protection measures, may personal information handlers handle sensitive personal information." [quotation from an unofficial translation as there is not an official translation at this time.] As sensitive data, the individual's specific consent is required.

Legal Bases

1. Why is there no legitimate interest in PIPL?
The Chinese legislator made that decision. We only know legitimate interest has not figured in the public drafts of PIPL.

2. Does sensitive personal information require explicit consent like under the GDPR?
Yes, consent needs to be provided for the handling of sensitive personal information under PIPL. This consent needs to be informed, voluntary, explicit, and needs to be provided separately from any other consents or permissions given by the individual. In addition, in order to handle sensitive personal information, there needs to be a specific purpose as well as a need to fulfill (*necessity check*).

3. Is it considered consent if an upstream company is given the consent and then information is passed to a supplier or would the supplier need to get consent as well?
The handling of personal information can take place on the legal basis that is used by the data handler (*the data controller*), whether that is consent or one of the other legal bases. Any entrusted person (*a data processor, vendor, or supplier*) can handle the data on that same legal basis, as long as they stay within the boundaries of the agreement with the data handler (*a data processing agreement*). Only if the personal information is transmitted to a different data handler, or if the purpose of the handling or the methods used change, renewed consent is required.

4. What would legal basis be for CCTV monitoring of entrances and exit points for security purposes?
Art. 26 PIPL restricts the use of CCTV and other image collection technologies or forms of identity recognition in public places. These can only be used to safeguard public security and as long as relevant State regulations are observed. The legal basis in this situation would likely be the statutory obligation provided in other laws. The data collected can only be used for safeguarding public safety except where the individuals separately consent otherwise.

5. If you are a university with students from China, could you rely on the contractual necessary basis? The university is offering an education to the student and they pay the university.
It is likely this is possible, given that the contract would be directly with the individual whose personal information would be handled.

6. For business to business purposes, would we need to put in a contract that the other party has obtained the rights of their employee to use their name and email address for the purposes of the contract?
We do not believe this to be a valid means of consent, given that the individual cannot make a voluntary and explicit statement. However, given that an entity must designate an individual to sign a contract and written contracts must be signed to be valid, it is likely that the provisions of contract law would apply.

7. In the absence of legitimate interest, do you think the legal basis of a contract with an individual (incl. HR) would be able to cover most of the processing operations in the employer context as a controller?
Yes, we believe this to be likely. All regular handling of personal information in an employment context, for example in order to pay salaries, to provide office software and to facilitate access to premises, could be covered under the employment contract. However, do bear in mind that full notice would need to be provided to the individual.

8. When handling personal information disclosed by the persons themselves or otherwise already lawfully disclosed, does that mean if the person registers for services using that personal information, that means they disclosed it themselves?
The voluntarily disclosed is connected with otherwise making information known publicly, so it is likely limited to public disclosure. However, registering for services sounds like consent or entering a contract.

Actors & Roles

1. What is a data controller called under PIPL?
The party responsible for the data handling operation, that we have come to refer to internationally as a data controller, is called a data handler under PIPL.

2. What is a data processor called under PIPL?
The party executing elements of the data handling operation on behalf and with instructions of another party is generally called a data processor, vendor, or supplier. Under PIPL, these are referred to as entrusted persons or entrusted parties.

3. PIPL requires the data handler to approve the use of trusted persons or parties by their own trusted parties or persons. Would a data handler be able to give general approval, or should each new trusted party or person be pre-approved separately?
It is not specified in PIPL in what ways the data handler can give their consent or approval for the use of further entrusted parties or persons other than that consent must be obtained.

4. Do vendors/processors need to register for processing personal data?
No, there is no such requirement included in PIPL.

5. Is separate consent required when data is transmitted from a data handler (*controller*) to an entrusted party or person (*processor*), even within China?
No, the transmission of personal information to an entrusted party or person is not subject to separate consent. Such consent might be required if the entrusted party is outside of China. In this regard, please also refer to Q43.

6. Is the DPO requirement on both data handler (controller) and also trusted parties?
No. A DPO (under PIPL: a personal information protection officer) need only be appointed by the data handler, from the moment the data handler reaches a yet-to-be-defined quantity of personal information that is handled. The DPO shall act both as an internal supervisor for the correct handling of personal information and be responsible for the implementation of data protection measures.

7. Is it possible to have a DPO in Europe? Are there any other specific requirements to take into account?
PIPL does not provide any details on the position, location, or competences of the personal information protection officer. Given that it is allowed to handle personal information in China without an establishment (but with the appointment of a representative), it can be assumed that it is possible that the personal information protection officer could also be located outside the country. Furthermore, given the need to supervise the data handling operations in China, it may be expected that the appointed person is competent in a Chinese language, but PIPL does not state so.

8. Must the representative appointed in China be a person, or can they be a company as well?
Based on the text of Art. 53 PIPL, a Handler outside China must establish an entity or appoint a representative located within the People's Republic of China to handle data protection measures. The name and contact information must be registered with the authorities. They do not specify that "representative" is a person or organiation. If they intend to follow GDPR, it could be either. If they intend it to be a natural person, they need to clarify it.

9. Are any further details available on the requirements for the representative, as well as for example as to their liability?
No. At this time, no further details are available. The liabilities for individuals in Art. 66 stress that individuals in charge or directly liable for personal information handling may be penalized. It does not explicitly state that representatives would be liable.

10. To which authority or authorities do details of the DPO and the representative need to be notified?

At this time, no specifics regarding the notification of a DPO and/or representative have been released. The law prescribes notification shall take place to the "departments fulfilling personal information protection duties and responsibilities.". We assume this will in any case include the Cyberspace Administration of China (CAC), but will add further details once they are released.

11. When will this contract form be out? Can this satisfy the 'separate consent' requirement, as when obtaining separate consent for cross-border transfers, sharing PI with third parties and processing of sensitive PI?

We do not know when the authorities will issue the approved templates. We also don't know if it will be strictly a B2B form (expected) or can involve data subjects themselves (unexpected). Under GDPR, data subjects cannot sign the standard contractual clauses as they are neither controllers nor processors. Thus, it is highly likely whatever approved contract is issued, it is intended to address data handlers and trusted parties.

Individual Rights

1. Do the rights apply retroactively or just future data?

PIPL does not provide a timeline along the concept of CCPA which specifies a 12 month lookback period for individual rights. Without such a specific inclusion, all personal information held by a data handler on or after 1 November 2021 that is in scope of PIPL, will also be subject to the individual rights.

12. How does the data retention period impact marketing databases? For marketing communications where an individual has affirmatively "opted-in," is it acceptable to continue to process the personal data until the individual "opts-out"?

That depends on for which purpose the initial opt-in consent was obtained. Data handlers are required to delete personal information once the handling purpose has been achieved - for example, if the person made a purchase following a marketing campaign. Furthermore, any change of the purpose, handling method (which may also include the use of a new type of database), or categories of handled personal information, means that new consent needs to be obtained.

13. Is anonymization allowed in place of deletion?

Yes. PIPL does not apply to anonymized data, which means any personal information handled prior to the anonymization would be out of scope. However, the bar for anonymization under the law is high and goes beyond the process of de-identification. For

anonymization to be successful, it should become impossible to "distinguish specific natural persons" - in order words: to be able to single someone out of a dataset, by whichever characteristics. Furthermore, the process should be irreversible, making it impossible to restore a dataset to its original state.

14. In relation to deletion, what if the organisation is required to keep records under their own country archiving laws, is there a carve out for an ability to retain information for that purpose?

Both Art. 19 PIPL (data retention) and Art. 47 PIPL (deletion) require data handlers to stop handling personal information once the purpose is achieved. To this end, the retention period must be set to the shortest possible time. However, there is a general exception to this if laws or administrative regulations provide otherwise. PIPL does not specify that this exception only applies to Chinese laws.

15. Is there more information on data subject private right of action?

The only information we have at this time is that Art. 50 allows individuals whose requests for individual rights are declined, to file a lawsuit in the people's court. It would be impractical to file suit if the request is denied because there is no data, so this relates to denying rights where there would be no legitimate reason to deny.

16. What about claims needed for actuarial reserves?

There is no specific carve-out in PIPL for personal information that may be needed as part of court proceedings or for an actuarial reserve. However, if this can be covered by a legal obligation in a country of establishment of the data handler, it is likely personal information could be handled for such a purpose.

Notice

1. Must PIPL terms be in Chinese?

Under Art. 17 PIPL, notice shall be provided in clear and easily understood language. Given that for PIPL to apply, the data handling will take place in China or is targeted at people in China, it is safe to assume that a notice under PIPL should at least also be provided in one or more Chinese languages. [The question asks about terms, we responded related to notice. Terms of use are not addressed in PIPL. In general, to hold individuals accountable to legal terms, they should be in the individual's language where the services are targeted.]

2. Does the notice require active consent?

No. Notification is a one-way street. The responsibility lies fully with the data handler.

3. Can the notice be included in a privacy policy or terms of use?

Although the requirements under PIPL are not as strict as the ones under GDPR when it comes to how the notice is provided, it is clear from Art. 17 that a full notice needs to be provided to individuals in clear and easily understood language. This implies the notice cannot be written in legal terms. Including it in your publicly posted privacy policy should be fine, as long as your "policy" is your privacy notice. It has been recognized for quite some time that privacy notices should not be included in terms of use for a website. The best practice would be to separate privacy from terms of use to ensure that notice is clear and not buried in other provisions. This may be different for mobile app terms.

4. What constitutes a "transfer"? Is accessing someone's data in the cloud a transfer? If a person is sitting in China and enters data on a website based outside China, is that a data transfer?

Like most data protection laws, PIPL does not include a definition of what constitutes a transfer. The law in Chapter III speaks about the cross-border provision of personal information, which would include anytime personal information crosses the border of the People's Republic of China, either physically or digitally. Accessing data in the cloud could be a transfer, depending on where the cloud servers and the individuals accessing the data are located. If all are still in China, there would be no data transfer. If the individuals accessing the data or the cloud servers are located abroad, this would constitute a data transfer.

Likewise, if the data being entered is personal information, it could very well be a data transfer, or rather a cross-border provision of personal information. However, to what extent this data handling operation would be covered by PIPL would also depend on who is entering the information and for which purpose this is done.

5. Would a US-style privacy policy (as opposed to an EU-style privacy notice) be sufficient for consent to transfer data outside of China? How would consent work for data transfers under PIPL?

Perhaps. Notice to be provided under PIPL for cross-border transfers need to be specific and fully informed, as explained above and separate from other consents. However, consent in itself does not appear to be a valid legal basis for data transfers out of China. One of the mechanisms described in Art. 38 PIPL (security assessment, standard contract, or certification) needs to be used. We expect further clarification for cross-border transfers.

6. For the purposes of cross border transfers, is de-identified personal information caught under Chapter III PIPL?

Yes. PIPL fully applies to de-identified personal information. Only once information is fully anonymized, is it out of scope of the law.

7. Can you be a Critical Information Infrastructure Operator if you transfer more than 1TB of personal information and/or about more than 500k individuals?

It's perfectly possible these numbers would indeed be within the limit of what is considered as a Critical Information Infrastructure Operator. However, at this time we do not know for sure what the qualifying criteria are yet. Further guidance on this definition - and the exact consequences of such a designation - are yet to be released. We will add further details to this Q&A once they become available.

8. If you handle data based on a legal basis (such as human resources management), can you rely on that legal basis for a cross border transfer, or do you have to obtain consent?

This is as yet unclear. Looking at the various translations of PIPL, a distinction seems to be made between the providing personal information to another party (e.g. in Art. 23, 38 and 39) or entrusting it to another party or person (Art. 21). This *could* mean that only the provision of personal information to another party outside of China would be subject to separate, individual consent (which would be comparable to a controller-to-controller transfer). Entrusting the data to another party (a controller-to-processor transfer) would then not be covered by the requirements of Chapter III PIPL. However, we need to await further guidance from the Chinese authorities for confirmation.

9. How do you think the cross-border requirements might apply to information collected directly from data subjects in China to an entity in another country? Would the foreign entity need the certification or security assessment?

No. The obligations to pass the certification or security assessment are imposed on the data handlers, not on the recipient of the data outside China. Under Chapter III on cross-border transfers, the law does not address the scenario where a natural person would directly provide their data to a foreign entity. Thus, that seems to fall under the bases of processing information in Art. 13 PIPL (consent, contract, etc.).

This is reminiscent of the recent guidance under GDPR that entities directly subject to the law are not required to have standard contractual clauses in place for cross-border transfers.

10. Is an exchange of emails typically considered to be a data transfer?

Yes, in principle exchanging emails and other types of messages with natural persons in other countries would cause data transfers to take place on the side of the communications service providers.

11. Would PIPL accept data transfers on the basis of EU BCRs or APEC CBPRs?

No, not at this time. However, the law explicitly leaves open the possibility to conclude treaties or international agreements that contain relevant provisions for international data transfers.

12. Will the cross-border transfer requirements also apply to setting cookies on websites? If so, on what legal basis could the transfer take place?

Yes, it is likely that cookie and tracker data is also seen as cross-border provision of personal information. Which of the three legal bases could be the most appropriate is hard to say at this time, given no details are known for any of them. It is likely that for the cross-border provision of cookie and tracking data separate individual consent is required, since the data will (also) end up with a different data handler. Please also see Art. 24 on automatic decision-making for information pushing or commercial marketing: additional notice is required or a convenient method to opt out.

13. Do you have any sense of whether keeping data local and then sending out a "copy" of the data similar to how some companies comply with Russian law be permitted ?

Perhaps. Where certain entities have a requirement to store data in China, like those who handle large volumes (Art. 40 PIPL), there is also the statement of where it is truly necessary to provide information to parties abroad, they must pass the security assessment. Whether the security assessment includes a determination of whether the cross-border transfer is truly necessary, is another matter. So, it is not just a matter of copying the data, it is a matter of meeting the requirements.

Browsers & Cookies

1. Do you have any indicators on how Global Privacy Control in certain browsers is to be handled? Is GPC an automatic opt-out of sharing personal information?

Global Privacy Control is an initiative to respect certain browser settings for opting in to, or opting out of, the use of cookies and trackers on a website. Whether this technology will be extended to cover PIPL is at this time unknown. In general, please note that PIPL requires an opt-in system for cookies and trackers, based on fully informed, explicit, active and separate consent that meets the requirements of Art. 14 PIPL. Only essential cookies can be seen as exempted from the consent requirement, based on Art. 16 PIPL.

Sanctions & Enforcement

1. How will China determine what constitutes a "grave" violation of PIPL?

We do not know at this time. No specifics have been included in the law or released otherwise.

2. I've heard different interpretations about whether the 5% of annual revenue is revenue in China or global. Your thoughts?

We do not know at this time. No specifics have been included in the law or released otherwise.

Other

1. How does PIPL impact the recent China Cybersecurity law?

The entry into force of PIPL does not change the application of other Chinese laws, like the China Cybersecurity Law. The obligations of the various laws will need to be respected.

2. Do you have any insight as to why PIPL has afforded 2 months to comply rather than the period afforded for GDPR, given there is so much wait and see (transfer security assessment templates, specialist body certification, large quantity). It feels impossible to comply without the details?

The details of the Parliamentary debate are unknown, and thus we have no insight on why the Chinese authorities chose a very limited transition period. It is true a lot of details are unknown at this time, but that will likely be true for most open norms-based data protection laws around the world. Our recommendation is to comply with the provisions of PIPL to the best of your abilities, and to properly document your considerations and decisions on

elements of the law that are not completely clear at this time.

3. How much bandwidth outside of China do they have to enforce?

We should not underestimate the capabilities of the Chinese authorities to enforce PIPL. It might be hard to directly impose a monetary penalty on companies without establishments or representatives in China, but the law also foresees the possibility of sanctions of a personal nature or that might impact the permissions to do business in China.

4. A lot of companies started to use biometrics in place of key cards to enter business establishments. Would PIPL impact this trend as well?

Any use of sensitive personal information will need to meet the requirements of Articles 29 - 32 PIPL. This means that there should be a specific purpose as well as sufficient necessity. A necessity check for the use of biometrics for identification will therefore need to be conducted.