

2021 (No. 15 issue)

September 2021

China accelerates personal data protection

Contacts

China

Martin Ng
Managing Partner
martin.ng@wts.cn
+ 86 21 5047 8665 ext.202

Maggie Han
Partner
Maggie.han@wts.cn
+ 86 21 5047 8665 ext. 206

Ened Du
Associate Partner
ened.du@wts.cn
+ 86 21 5047 8665 ext.215

In brief

- » China's first dedicated law on personal data protection will take effect from 1 November 2021. It governs both onshore and offshore personal data processing parties.
- » Business operations engaging in the processing of personal data generated from or collected in China should be reviewed for compliance purposes.

Feedback

WTS – strong presence in about 100 countries / regions

Albania • Angola • Argentina • Australia • Austria • Azerbaijan • Belarus • Belgium • Bolivia • Bosnia-Herzegovina • Brazil • Bulgaria • Cambodia • Canada • Chile • China • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Egypt • Ecuador • El Salvador • Estonia • Finland • France • Germany • Ghana • Greece • Guatemala • Honduras • Hong Kong • Hungary • India • Indonesia • Iran • Ireland • Israel • Italy • Japan • Kazakhstan • Kenya • Korea • Kuwait • Laos • Latvia • Lebanon • Lithuania • Luxembourg • FYR Macedonia • Malaysia • Malta • Mauritius • Mexico • Mongolia • Montenegro • Morocco • Netherlands • New Zealand • Nicaragua • Nigeria • Norway • Oman • Pakistan • Panama • Peru • Philippines • Poland • Portugal • Qatar • Romania • Russia • Saudi Arabia • Serbia • Singapore • Slovakia • Slovenia • South Africa • Spain • Sri Lanka • Sweden • Switzerland • Taiwan • Thailand • Tunisia • Turkey • Turkmenistan • UK • United Arab Emirates • Ukraine • Uruguay • USA • Uzbekistan • Venezuela • Vietnam

2021 (No. 15 issue)

September 2021

In detail**» New law on personal data protection**

China passed its landmark privacy protection law, the 74-article “*Personal Data Protection Law*” (hereinafter as **PDPL**) on 20 August 2021. The new law will take effect from 1 November 2021 and will have a global impact.

Affected parties

PDPL has collectively named all the personal data processing parties as “*personal data processors*” (hereinafter as **PDPs**). PDPs cover individuals and corporations engaging in the processing of personal data generated from or collected in China.

Further, the law governs not only onshore but also offshore PDPs which sell products to or provide services to personnel in China, engage in analyzing or evaluating personal behavior in China or receive personal data from China.

Personal data

PDPL has defined personal data as “*all kinds of data related to the identified or identifiable natural persons stored electronically or by any other means, but excluding those anonymous data*”.

Specifically, it has laid out provisions for sensitive personal data which, in case of leakage or misuse, may potentially damage personal dignity, personal safety, and property safety, e.g. biometric identification, religions, special identity, medical health, financial accounts, and location tracks, as well as the personal data of minors under the age 14.

Personal data processing acts

According to the new law, the term “*processing*” is meant to cover the wide range of acts concerning personal data, from collection, storage, usage, editing, transmission, provision, disclosure to deletion.

Further highlights

The details of other provisions of PDPL are summarized and enclosed overleaf under the following headings:

- A. Guiding principles
- B. Safe harbor
- C. Requirements on personal consent
- D. Multiple personal data processors (PDPs)
- E. Rights and obligations in personal data processing
- F. Sensitive personal data
- G. Cross-border provision of personal data
- H. Rights of individuals
- I. Obligations of a personal data processor (PDP)
- J. Penalty clauses

2021 (No. 15 issue)

September 2021

WTS China's observation

This legislation inscribes China's first comprehensive legal attempt to define personal data and regulate the processing of them, in the existence of other legislations concerning data security, like Cybersecurity Law, the Civil Code, the Data Security Law, and the E-Commerce Law.

Business communities should note its global impacts as it governs the processing of personal data not only in China but also outside China. It mandates that domestic regulators' approval is required even though the transfer of personal data overseas is to meet any judicial or legal obligations.

Further, the definition of personal data is so broadly set that it covers also some other information particularly sensitive to the interests of the persons, e.g. location tracking or religion belief. In other words, personal data collection would better be limited to the minimum extent necessary for the operation.

Business operators should review the regulatory and commercial impacts caused by the new law for the obligations, systems, and compliance procedures imposed on them as a PDP. E.g. an internet sales platform operator should review if its customized sales proposal generated from an automated decision-making process is accompanied also by a non-customized option; a retail outlet operator should check if its collection of personal data via an image capturing equipment is legal or not.

Special attention should also be paid to the harsh and onerous requirements set for cross-border transfer of personal data from China. It is possible that some offshore operations could fall into the restriction scope and may need to meet the new requirements: e.g. offshore shared service centers (SSC) and marketing hubs entailing personal data transmission from China, or an offshore intranet infrastructure in the possession of a large amount of personal data generated from China.

Click below to read China news on personal data protection:

- *"Musk confirms Tesla will store Chinese data locally"*, 26 September 2021, Shanghai Daily
- *"Three app firms face scrutiny over data security"*, 6 July 2021, Shanghai Daily
- *"China's Didi refutes rumors about service suspension"*, 18 July 2021, Shanghai Daily

Abstract of China's "Personal Data Protection Law" (DPPL)**A. Guiding principles**

Personal data processors (PDP) are required to observe these guidance principles:

1. Ensuring the process is legal, reasonable, and reliable, without involving any misleading, fraudulent, or coercive measures;
2. Obtaining a discrete approval from the persons involved;
3. Ensuring succinct transparency on data usage and processing methods;
4. Safeguarding the quality and security of personal data in the process;
5. Avoiding any acts against state security and public interest;
6. Limiting the quantity of personal data processed to the extent possible; and
7. Limiting the storage period of personal data to the shortest time possible.

B. Safe harbor

PDPL has indicated the following situations *allowable* for personal data processing.

1. It is conducted after obtaining consent from the persons concerned;
2. It is necessary for establishing a commercial or employment contracts;
3. It is necessary for fulfilling mandatory statutory or official duties in China;
4. It is necessary due to public hygiene or emergency incidents;
5. It is necessary for news reporting and public supervision;
6. It concerns only the personal data already made public by the individuals concerned or by other legal means; or
7. Other circumstances prescribed by China's laws and regulations.

To business operators in general, the first three types of personal data processing could be the most common.

C. Requirements on personal consent

1. The data processor shall seek personal consent from the individuals concerned, based on full disclosure, under a voluntary situation, and in a discrete or written format (except situations from [2] to [7] mentioned above);
2. The data processor shall re-seek personal consent if the data usage scope has changed;
3. The data processor should allow the individuals to withdraw their consent any time without setting any conditions or hassles;
4. The data processor cannot refuse to sell products or provide services to the individuals on the ground that they have disapproved or withdrawn their consent for processing their personal data;
5. The data processor is required to disclose to the individuals its identity, contact methods, data usage scope, and data storage period;
6. The data processor is required to notify the individuals when it has processed their personal data without their prior consent due to emergency situations.

2021 (No. 15 issue)

September 2021

D. Multiple person data processors (PDPs)

PDPL has laid out provisions governing four situations in which multiple PDPs will be involved, including:

1. **Co-processing:** If two or more PDPs are involved, they need to agree contractually on each other's rights and obligations. The individuals can exercise their rights and claims against any of them, holding them responsible for joint and several liability for any damages caused.
2. **Outsourcing:** The PDP, if outsourcing its data processing tasks to other agents, is required to agree with them contractually on the purposes, time limit and method, type of personal data, protection measures, as well as the rights and obligations of both parties, and to supervise the acts of the agents. The agents are required to return or delete the personal data, once its outsourcing contract ceases to be effective.
3. **Restructuring:** The PDP, if needed to transmit its personal data to others in time of restructuring like merger, division, dissolution, or bankruptcy, is required to inform the persons concerned of the changes. The data recipients will be held responsible for their obligations as a PDP, and are required to refresh the consent-seeking process if they intend to process the personal data in a manner different from that of the original PDP.
4. **Transmission:** The PDP, if intending to transmit personal data to others, is required to seek personal consent from the individuals concerned; the data recipients are required to re-seek the individuals' consent if they have changed the original processing purposes and scope.

E. Rights and obligations in personal data processing

PDPL has set out the rights and obligations for personal data processors (PDPs):

- The PDPs shall ensure transparency, fairness, and impartiality when using personal data in an automatic decision-making process; for any customized sales proposals provided to individuals, it should also provide non-customized options and a convenient means for their rejection.
- The individuals have the right to seek an explanation on or reject a decision made only through an automatic decision-making process.
- The PDPs shall not make public any personal data, unless with the individual's consent.
- The PDPs, if installing any image capturing and personal identification equipment in public venues for collecting personal data, should use them only for maintaining public security; it should also display a conspicuous sign for the equipment.
- The PDPs may process the personal data already made public by the individual concerned or by other legal means but must still seek personal consent from the individual if it has a major impact on his/her rights and interests.

2021 (No. 15 issue)

September 2021

F. Sensitive personal data

PDPL has set out separate provisions governing the processing of sensitive personal data:

- It should only be conducted for a specific purpose and sufficient necessity, and under strict protection measures;
- It shall be subject to the individual's consent, and even in writing if the regulations require so in certain cases;
- It should be made known to the individuals on the necessity and the impacts;
- It should be subject to the consent of the minor's parents or other guardians if it processes the personal information of a minor under the age of 14. It should be conducted under special measures formulated by the PDP specifically for the personal data of minors under the age of 14.
- It should be subject to relevant permits or other restrictions if such provisions prevail.

G. Cross-border provision of personal data

From China's perspective, a cross-border provision of personal data from China to overseas is considered as a sensitive act.

PDPL has spelled out lengthy and stringent conditional provisions on such an act. PDPs are advised to exercise pragmatic measures to ensure meeting ALL the following requirements before transmitting personal data from China to overseas:

1. It shall be put to a security evaluation by the Cyberspace Administration of China ("CAC");
2. It shall be certified by a specialized body on its effectiveness in data protection;
3. It shall establish a contract with the overseas recipient using CAC's standard contract template, setting out the obligations and interests of both parties;
4. It shall meet the conditions prescribed by China's laws and regulations, and CAC's provisions;
5. It shall comply with any international treaties or agreements concluded with or acceded to by China for the provision of personal data outside China;
6. It shall exercise necessary measures to ensure that the overseas personal data recipient can also meet China's personal data protection standards;
7. It is subject to the individual's consent, and the PDP in China has to inform the individual concerned of the details of the cross-border transmission;
8. It is prohibited to transmit personal data overseas if the data size has reached the limit prescribed by CAC, and all personal data generated and collected in China shall be stored in China; If it is really necessary for the transmission to overseas, it should be subject to CAC's evaluation first;
9. It will be subject to the approval by China's relevant authorities if such a personal data transfer to overseas is for fulfilling any obligations under the international treaties and agreements concluded or acceded to by China; no such transmission is allowed to any foreign judicial or law enforcement authorities unless the said approval is granted.
10. No personal data transmission can be made to any overseas organizations or individuals blacklisted by CAC for their records of infringing on personal data laws or endangering national security and public interests.
11. No personal data transmission can be made to any countries or regions blacklisted by China for their discriminatory, prohibitive, restrictive, or other similar measures against China in personal data protection areas.

Notably, it would require exhaustive review and application efforts to achieve a cross-border transmission of personal data, to the extent that one may call it discouraging.

H. Rights of individuals

It is noteworthy of the rights of individuals that a PDP should be prepared to respect:

1. The right to know and make decisions on the processing of his/her personal data, and the right to restrict or refuse others to process his/her personal information, unless otherwise provided for by the laws;
2. The right to consult or copy his/her personal data from a PDP, and the right to request the transmission of his/her personal data to a PDP designated by him/her;
3. The right to request corrections or supplements, if finding his/her data is incorrect or incomplete;
4. The right to request deletion to his/her personal data when the need for the data process no longer exists, the PDP ceases to operate or has violated data protection laws, the data storage period has expired, or the laws require the deletion.
5. The right to request a PDP to explain its personal data processing rules.
6. The right to consult, copy, correct and delete the personal data of his/her close relatives who have deceased; and
7. The right to file a lawsuit with a court against a PDP who refuses an individual's request for exercising his/her rights.

I. Obligations of a personal data processor (PDP)

1. Set up a personal data management and protection system, for persona data processing, classification, security, authorization, training, and emergency plans;
2. Nominate a *personal data protection officer* for supervising all personal data processing, where the size of the personal data processed has reached that specified by CAC; make public and submit his/her name to the personal data protection authorities;
3. For any PDPs outside China in cross-border data transmission cases, nominate an organization or a representative in China responsible for personal data protection matters; submit its name and contact methods to China's personal data protection authorities;
4. Conduct regular compliance audits on the processing of personal data;
5. Conduct an impact assessment on personal data protection matters; keep a record of the treatments; maintain the report for at least three years;
6. Exercise remedial measures and notify the authorities and the individuals concerned for any personal data being leaked, tampered with or lost;
7. The said notification to individuals can be waived, if the PDP has taken effective remedial measures for the incidents. Yet, if the personal data protection authorities believe that harm is caused, they may require the PDP to notify the individuals concerned.
8. Assume the following additional obligations, if a PDP provides important Internet platform services with a large number of users and complicated business:
 - a) Establish a supervision body composed of external members to supervise personal information protection;
 - b) Formulate rules and standards, based on the principles of openness, fairness, and impartiality, for personal data processing and protection;
 - c) Ban any vendors of products or services from using the platform if they have seriously violated the regulations; and
 - d) Publish social responsibility reports regularly on personal data protection matters for social supervision.
9. Where an agent is entrusted with the task of personal data processing by a PDP, it should take necessary measures to ensure data security and assist the DPP to perform its obligations.

2021 (No. 15 issue)

September 2021

J. Penalty clauses

The consequences of violation to PDPL could be serious business disruption, penalty, and discrediting. The penalty will be imposed in the following sequence:

1. In a minor case, a warning for correction will be issued by a local authority, related income will be confiscated, and the application programs concerned will be temporarily or permanently suspended from usage;
2. If a correction is not made, a fine up to CNY 1 million (roughly USD 155,000*) will be imposed on the entity concerned, and a fine to the personnel in charge in the range of CNY 10,000 (about USD 1,550*) to 100,000 (about USD 15,500*); or
3. In a very serious case, a warning for correction will be issued by a provincial or above authority governing personal data protection, related income be confiscated, a penalty of max. CNY 50 million (about USD 7.75 million*) or 5% of last year's revenue will be imposed, related business will be suspended or halted, related licenses or permits will be suspended or revoked, a penalty will be imposed to the personnel in charge in the range of CNY 100,000 (about USD 15,500*) to 1 million (about USD 155,000*), and their appointment to any position of directors, supervisors, senior managers, or personal data officers in China will be prohibited.

Further, the violation record would be posted to the credit systems accessible by the public.

** The CNY to US exchange rate stands at 1 to 0.155 on 28 September 2021*

2021 (No. 15 issue)

September 2021

WTS

China Contact

Martin Ng
Managing Partner
martin.ng@wts.cn
+ 86 21 5047 8665 ext.202



Germany Contact

Ralf Dietzel
Partner
ralf.dietzel@wts.de
+49 (0) 89 28646 1745



Maggie Han
Partner

+ 86 21 5047 8665 ext.206



Xiaolun Heijenga
Partner
xiaolun.heijenga@wts.de
+ 49-69-1338 456 320



Ened Du
Associate Partner
ened.du@wts.cn
+ 86 21 5047 8665 ext.215



WTS China Co., Ltd.

Unit 06-07, 9th Floor, Tower A, Financial Street Hailun Center,
No.440 Hailun Road, Hongkou District,
Shanghai, China 200080
T: +86 21 5047 8665
F: +86 21 3882 1211
www.wts.cn
info@wts.cn



Disclaimer

The above information is intended for general information on the stated subjects and is not exhaustive treatment of any subject. Thus, the content of this Infoletter is not intended to replace professional tax advice on the covered subjects. WTS China Co., Ltd. cannot take responsibility for the topicality, completeness or quality of the information provided. None of the information contained in this Infoletter is meant to replace a personal consultation. Liability claims regarding damage caused by the use or disuse of any information provided, including any kind of information which is incomplete or incorrect, will therefore be rejected. If you wish to receive the advice of WTS China Co., Ltd., please make contact with one of our advisors. All copyright is strictly reserved by WTS China Co., Ltd.