DS NEWSLETTER savoir faire
NEWSLETTER – LEGAL INFORMATIONS
PROPOSED BY DS AVOCATS

How's your privacy policy?

CHINA

Nowadays, organizations mostly cannot avoid processing personal data in their daily operation. It could be the personal data of internal employees, consumers, clients and business partners. In particular, B2C enterprises may have already updated their privacy policies for many times due to the ever-updating requirements by law and regulations on personal data protection.

Despite the way of collecting personal data, a privacy policy which meets legal requirements and be updated regularly should be provided to individuals ("Data Subjects") before any collection and/or processing starts. For example, data controllers may plan to collect personal data by online channels via webpage, application, Wechat mini-program or by offline channels via applications forms etc. It should be noted that how personal data is collected will not exempt data controllers from the obligation of information, i.e., the privacy policy.

In the 3rd year of the *PRC Personal Information Protection Law*, we have seen that enterprises pay more attention to personal data protection than they did before. However, the ever-updating legal requirements make data controllers keep refining their data protection measures. One of the important tasks, is to have an updated and qualified privacy policy. In practice, there are still cases where a makeshift privacy policy is provided with vague clauses, or privacy policy is absent at all. Of course, these makeshift privacy policies would not delivery a satisfactory result to the data controllers; in worse cases, they may risk the data controllers and lead to high price for non-compliance.

Last year, a Chinese well-known academic group was fined RMB 50 million by the Administration of Cyberspace of China for illegal processing personal data and violating the PRC Cybersecurity Law and the PRC Personal Information Protection Law. To be more specific, it operated 14 applications with makeshift privacy policies or some were totally without any privacy policy. As a result, the data controllers were fined for collecting unnecessary categories of personal data without consent, without disclosing/providing personal data processing rules, failing to provide the right of deregistration, and failing to delete the personal data etc.

To avoid the risks, below please see some tips of necessary procedures on how to make a good privacy policy (B2C scenarios):

- √ Step 1: Know ALL of your business scenarios processing personal data and what exactly categories of personal data are needed.

  This step is to collect facts related to personal data processing. Firstly, business department (and/or others whose duties are related) should describe in detail the data collection and processing activities intended by the data controller. In other words, it should reflect the real purposes, method of processing and scope of categories of personal data to be collected. Data minimization should be followed to exclude unnecessary categories of personal data. To that end, data controllers should distinguish the categories of personal data collected for necessary functions (core product/service) from those for the other extended functions of products/services.

  An official guide for mobile Internet applications released in 2021 could be a good reference, namely, *Scope of Necessary Personal Information for Common Types of Mobile Internet Applications.* Per this Guide, Data Subjects should have the right to refuse providing unnecessary categories of personal data and such refusal should not prevent Data Subjects from using the core/basic function of the products/services provided by the data controller.

√ Step 2: Make a privacy policy with a balance between business target and compliance requirements.

The privacy policy draft should be reviewed comprehensively by professionals, then to be finalized and confirmed by the full team members (despite internal or not, including the team who know legal requirements, business targets, actual data processing activities, and technical /IT professionals who provide necessary assistance in security aspect). This step should be managed by data controllers more carefully if they are processing sensitive personal data and/or where cross-border data transfer may occur.

√ Step 3: Grow the privacy policy as a living document instead of letting it rust into risks.

Data controllers' obligation of information to Data Subjects dose not end upon disclosing of a privacy policy, but it substantially starts since then. In practice, sometimes it is ignored by data controllers that privacy policy needs to be maintained and updated regularly accordingly to the applicable laws. Data controllers should supervise the data processing activity and adjust the privacy policy and/or the activity when needed. In addition, when update/amend a privacy policy, there are also rules to follow of how to display the previous versions and the updated ones.

Under the current legal environment, it would be difficult to justify an illegally processing of personal data, especially regarding obtaining consent via privacy policies. After all, answers and approaches are all provided by national standards. We list some of the latest ones as follows for your reference:

Code	National Standard Name	Release Date	Effective Date
GB/T 43506-2023	*User Personal Information Protection Requirements*	2023-12-28	2024-04-01
GB/T 42574-2023	*Implementation Guidelines for Notices and Consent in Personal Information Processing.*	2023-05-23	2023-12-01
GB/T 42582-2023	*Personal Information Security Testing and Evaluation Specification in Mobile Internet Applications（App）*	2023-05-23	2023-12-01
GB/T 41391-2022	*Basic Requirements for Collecting Personal Information in Mobile Internet Applications*	2022-04-15	2022-11-01

Meanwhile, we also summarize some "*Don'ts*" based on administrative punishment cases on personal data processing in the recent years and our experience as follows for your reference:

- No privacy policy is provided; or, the link of privacy policy is provided but it does not work.

- Privacy policy is displayed and accessible, but it does not include/clear as to:
  - the rules of collecting personal data;
  - the basic introduction of the controller;
  - Effective term/date of the privacy policy;
  - Notice of update (if any);
  - Personal data processing rules (purposes, methods and scopes) of the 3rd party SDK (Software Development Kit); or,
  - Retention period and disposal method after the retention period.

- Privacy policy is displayed and accessible but it is not:
  - in simplified Chinese;
  - in simple language (easy to read); or,
  - easily accessible by Data Subjects (more than 4 clicks needed in mobile applications).

- Related to Data Subjects' Rights:
  - Fail to respond Data Subjects rights or delay in response to Data Subjects;
  - Fail to provide complaint channel or contact information to Data Subjects; or,
  - Deregistration right of the user account is not provided/provided but unreasonably complicated.

- Other scenarios:
  - The actual data processing activities do not follow the Privacy Policy and violate the principle of data minimization, necessary and transparency;
  - Sensitive personal data to be collected is not marked separately; and corresponding purposes, methods and scope of categories of processing sensitive personal data are not listed;
  - Providing personal data to 3rd parties without consent of Data Subjects or anonymization of personal data;
  - Collection and/or processing personal data before Data Subjects' reading the privacy policy and consent; or,
  - Personal data is not deleted after Data Subject's deregistration of the user account.

In addition to the above commonly seen violations, data controllers, especially those who process personal data via mobile applications and Wechat Mini-program, are advised to pay more attention to national standards as to requirements on collection and processing of personal data. More figures and detailed rules are provided regarding users' clicks, frequency of asking for consent of a certain processing scenario, and retention period, etc.

In a word, a trustworthy privacy policy not only respects the fundamental principles set by applicable laws, but also helps to realize business targets while lowering the impact to Data Subjects. Its main text will pass the information during the first interface shown to Data Subjects, and its key alerts will also remind Data Subjects when/shortly before important data processing activities occur. For example, pop-up notification shortly before collecting sensitive personal data (camera for facial recognition, microphone, providing GPS data and health data etc.) by mobile applications. The more personal data (especially sensitive personal data) a data controller wants, more efforts the data controller should put in the privacy policy and notices in personal data processing activities.

Ending remarks

A privacy policy is supposed to show the accountability of the data controller by notifying Data Subjects of personal data processing rules. Whenever being challenged by Data Subjects, data controller could use the privacy policy as the legal evidence to justify its processing of personal data. However, if a privacy policy is not fact-based and/or misleading, it could also be used by Data Subjects as documentary evidence to against the data controller in administrative complaint or other legal actions, which backfires the data controller.

For any additional information, please contact:

Isabelle DOYON
Associate - Shanghai Office
doyon@dsavocats.com

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

11, April 2024