Published on *The National Law Review* https://natlawreview.com

China Issues New Personal Information Protection Standard

Article By:

Yan Luo

Philippe Bradley-Schmieg

On January 2, 2018, the Standardization Administration of China ("SAC") released the final version of the national standard on personal information protection, officially entitled *GB/T 35273-2017 Information Technology – Personal Information Security Specification* (GB/T 35273-2017 ?????? ????????) (hereinafter "the Standard"). The Standard will come into effect on May 1, 2018.

As highlighted in our previous coverage of drafts of the Standard (see here and here), although it is nominally a voluntary framework, the Standard effectively sets out the best practices that will be expected by regulators auditing companies and enforcing China's existing (but typically more generally-worded) data protection rules, most notably the 2016 Cybersecurity Law. Drafts of the Standard — even prior its finalization — have also in some cases been the basis for non-compliance remediation plans and undertakings agreed between companies and the Cyberspace Administration of China ("CAC") following CAC audits, as we reported here.

The Standard applies to "personal information controllers," namely any private or public organization that has "the power to decide the purpose and method" of processing personal information. This is seemingly modeled on European law's "data controller" concept.

The Standard regulates the use of "personal information" by these controllers, a term largely aligned with strict conceptualizations of "personal data" under the EU's General Data Protection Regulation ("GDPR"). Examples of "personal information" listed in an annex to the Standard include device hardware serial codes, IP addresses, website tracking records, and unique device identifiers, among other things. The definition of "sensitive personal information," however, takes a different approach to the GDPR: rather than applying only to specific types of data, the Standard takes a risk-based approach, defining "sensitive" personal information as any personal information which, if lost or misused, is capable of endangering persons or property, easily harming personal reputation and mental and physical health, or leading to discriminatory treatment. According to the Standard, this could, for example, include national identification card numbers, login credentials, banking and credit details, a person's accurate location, information on a person's real estate holdings, and information about a minor (under 14 years old).

Similar to general principles of most data protection laws, the Standard requires transparency, specificity and fairness of processing purpose, proportionality (use and retention of only the minimum

information necessary to achieve the stated purpose), security, risk assessment, and the respect of individuals' rights to control the processing of information about them. It also requires either consent from individuals, or reliance on a limited range of exceptions set out in the Standard, for the purpose of collection and processing of personal information.

This article looks at some of these aspects in more detail, including some of their key divergences from European data protection law, including the GDPR. (Please note that this is not an exhaustive description of the Standard, nor is it a detailed comparison with the GDPR.)

Consent and other legal grounds for processing

The Standard lays down a basic rule that the collection of personal information and its subsequent use should be affirmatively consented to ahead of time, with further (informed) consents being required for any activity exceeding the scope of the original consent.

For sensitive personal information, the informed consent must be clear and explicit, and the information to be provided must distinguish between the "core business functions" of the products or services being provided, and "other products or services, such as those that provide additional capabilities." If an individual refuses to consent to the ancillary uses of their data, the collector/controller may decline to provide the additional services, but may not cease or degrade the provision of core business products and services to that individual.

Where the data relates to a minor, explicit consent must be obtained from the minor's parent or guardian, unless the minor is at least 14 years old, in which case consent may also be obtained directly from him or her.

The Standard derogates from these consent requirements by including a number of non-consensual grounds for collecting and processing personal information. Analogues of several of those grounds can be found in the GDPR, but others are different, for instance, the necessity for troubleshooting products and services, or necessity for reporting by news agencies. Collecting information from public sources, such as news reports, also does not require prior consent. Some of the more permissive processing grounds found in GDPR Article 6 (for non-sensitive data) are absent, such as the necessity for the legitimate interests of the controller or a third party, even though the Standard's exceptions arguably cover some of the commonly seen examples of legitimate interests, including necessity to perform a contract.

As further described below, consent is usually also required to the sharing or transferring of personal information.

The Standard also imposes a requirement akin to the GDPR's "purpose limitation" requirement (namely, that all uses of the information, including secondary uses, should be reasonably connected with the original purpose of collection of the data, and should be reauthorized if that is not the case). It sets aside that principle for certain research and academic purposes, provided the personal information is de-identified in public disclosures about the research.

Notice

The Standard requires the inclusion of certain information in privacy notices, including but not limited to:

- For each business use: personal information collection and processing rules such as the collection method and frequency, place of storage, and frequency of collection;
- If data is shared, disclosed or transferred, the types of data involved, the types of the data recipients, and rights and obligations of each party;
- Data subject rights, and complaint handling;
- Security principles followed, and security measures implemented;
- Security risks that may exist after providing personal information; and
- The controller's "usual office location" and contact information.

The Standard does not explicitly allow such information to be omitted from notices if the individual already possesses it from other sources (*e.g.* from app pop-up notices, or through their regular dealings with the organization), unlike the GDPR. Privacy notices must be delivered to individuals "one by one," though if costs become too high or when there are significant difficulties, a public announcement is possible instead.

The Standard also requires cessation of processing to be notified to individuals, either individually or by a general announcement.

Rights of individuals

The rights conferred on individuals are similar to those under the GDPR, although:

- The Standard requires requests to be complied within less than 30 days (or other legally-stipulated period), whereas under certain circumstances the GDPR allows further extensions;
- The Standard includes a "straightforward account cancellation" right;
- The erasure right appears somewhat strengthened, through omission of exceptions found in the GDPR (which for example allows refusal of erasure requests in the interests of freedom of expression and information, or scientific research), and includes significant obligations to notify third parties of the erasure (and in some cases, order them to also delete the data). On the other hand, the right can only be invoked after processing violates applicable law or an agreement with the individual.
- The data portability right arises in a wider range of situations but is limited to certain information, such as health, education or occupational information.

Use of vendors/processors

Before outsourcing the processing of personal information, the Standard requires controllers to conduct risk assessments and ensure that the vendor (processor) would offer adequate security; once the subcontracted processing is underway, controllers must supervise the processors, including through audits and assessments. Processors must obtain controllers' permission before further

subcontracting the processing services.

Like the GDPR, processors must help controllers comply with data subject requests, and promptly notify controllers of security incidents. The Standard adds broader duties to promptly notify controllers when processors are "unable to offer an adequate level of security" or after they process the information entrusted to them other than strictly in accordance with the controller's requirements.

Data sharing

Unless the information is de-identified, prior notice and consent from individuals to the transfer or sharing of their data is required (distinct from the consent that covered the initial collection and processing of data), as is also required by China's Cybersecurity Law. By contrast, the GDPR does not strictly require consent to sharing of data. However, the GDPR and the Standard both suggest that the sharing be covered by some sort of prior risk assessment and mitigation exercise.

The Standard also sets out specific record-keeping obligations regarding the sharing or transfer of personal information, and an obligation on controllers to assume a degree of responsibility for any damage caused to individuals by the transfer or sharing of their personal information.

Alternative rules apply in respect of mergers, acquisitions, reorganizations or "other kinds of change," as well as to public disclosures of personal information. Public disclosures of biometric information are prohibited.

As with processing grounds, exceptions to the aforementioned sharing, transfer, and disclosure consent requirements apply, for instance, where the data was collected from public sources, or if the disclosure is necessary for criminal investigations.

Security and deletion

The Standard prescribes that controllers must (i) have internal procedures to grant access to personal information and authorize operations such as batch modification, copying and downloading; (ii) keep records of data processing; (iii) appoint a Chief Information Security Officer plus designated "key personnel" with leadership responsibility for information security; (iv) conduct periodic (at least annual) staff training; (v) conduct security testing before the release of products or services; and (vi) if the organization is large enough or processes information about more than 500,000 people (or expects to do so in the next 12 months), have a dedicated information security team. Individuals with access to large amounts of sensitive personal information must be subjected to background checks. In requiring these specific programs, the Standard is more granular than the GDPR.

Incident response

The Standard requires organizations to maintain information security incident response plans, undertake regular training and emergency drills (at least once a year), implement incident record-keeping and assessment, adhere to the CAC's "National Network Security Incident Contingency Plan" for notification of incidents to authorities, and notify cybersecurity incidents to affected individuals. Unlike the GDPR, no severity threshold or specific time period for reporting is expressly mentioned under the Standard.

Note that the Cybersecurity Law requires "network operators" to notify an incident to regulators and affected individuals when there has been actual or potential "leakage, damage, or loss" of personal

data (Article 42). It is not clear whether a data controller would be subject to this reporting obligation if the breach occurs within their processors' network, nor what kind of incidents may be counted as "potential" breaches.

Periodic data protection impact assessment

Finally, the Standard requires data protection impact assessments ("DPIAs"), which are not unlike those in the GDPR, although the GDPR is less specific about how frequently they must be conducted: under the Standard, DPIAs must be repeated at least annually, as well as when (i) new legislative requirements come into effect, (ii) business models, information systems or operational environments undergo a major change, or (iii) a significant personal information security incident occurs. The assessment reports must be "open to the public in appropriate form."

International data transfers

The Standard states at a high level that data controllers will need to go through a security assessment if they would like to transfer personal data out of China. More detail regarding cross-border data transfers are expected to be covered by separate regulations and standards.

National Law Review, Volume VIII, Number 25