Busting the myth: compliance with the ‘gold standard’ of the GDPR does not buy you a ‘free pass’ under China's new personal information guidelines

Hogan Lovells

November 2018

Overview and background

On December 29, 2017, the Standardization Administration of China ("**SAC**"), jointly with the PRC General Administration of Quality Supervision, Inspection and Quarantine ("**AQSIQ**", now part of the new super-regulator, the State Administration for Market Regulation or "**SAMR**"), issued the *Information Security Technology – Personal Information Security Specification* (GB/T 35273-2017, the "**Specification**"), which officially came into effect on May 1, 2018. The Specification supplements the broad principles set out in the *PRC Cyber Security Law*, effective on June 1, 2017 (the "**Cyber Security Law**") and provides detailed and practical requirements and examples with respect to the processing of personal information.

Although the Specification is only a recommended (as opposed to a mandatory) national standard, we still recommend full compliance with the Specification, given its practical value in terms of demonstrating a compliance culture in this area, and the fact that the authorities in China appear to be using it as a compliance yardstick in practice, and are holding companies in China to account for failing to comply with the Specification. This recommendation has taken on particular importance in the context of the current tensions in international trade, leading many multinationals to conclude that demonstrations of strict compliance in sensitive areas of Chinese regulations are as important now as they have ever been. The introduction of the Specification also comes at a time when public awareness of data protection appears to be on the rise in China, with consumers more likely to demand that their rights in personal data be respected.

This alert discusses what has changed or is new under the Specification, as compared to earlier non-mandatory guidelines also issued by SAC and AQSIQ, the *Guidelines on Personal Information Protection within Information Systems for Public and Commercial Services on Information* Security Technology ("**2013 Guidelines**"). We will also look at some of the differences between the Specification and the *General Data Protection Regulation* ("**GDPR**") (EU) 2016/679, made by the European Parliament and Council of the European Union and effective from May 25, 2018. Although the Specification purports to have used GDPR as one of its reference points, companies should not assume that compliance with the GDPR automatically implies compliance with the Specification.

Non-binding but highly influential and useful as a compliance tool

In common with the 2013 Guidelines, the Specification is not a mandatory national standard. However, the Specification goes a step further than the 2013 Guidelines in that it expressly says that it not only applies to the regulation of personal information processing activities by various types of organizations, but also applies to the supervision, management and assessment of personal information processing by regulators and third party assessment agencies. This has played out in practice and in terms of how the regulators have been applying the Specification.

In January this year, a well-known non-banking payment institution in China was reportedly summoned by the Cyberspace Administration of China ("**CAC**") for an interview due to "inappropriate" collection of users' personal information (by using pre-ticked consent boxes in its online T&Cs). Days later, the CAC decided that the manner in which the payment institution collected personal information was against the "spirit" of the Specification, and recommended that the institution should conduct a comprehensive internal review pursuant to the Cyber Security Law and rectify the position. This demonstrates that the Specification is indeed being used by the regulatory authorities when assessing whether a company complies with the provisions of the

Cyber Security Law and the relevant laws and regulations concerning the protection of personal information.

Looking beyond the data protection provisions found in the Cyber Security Law, the Chinese data protection regulatory landscape is notable for the proliferation in recent years of mandatory data protection requirements, such as the amendments to the *PRC Consumer Rights Protection Law* (the "**Consumer Protection Law**") introduced in 2014, provisions in the recently passed *PRC E-Commerce Law* and the complex array of laws and measures addressing online data collection in China. The data protection provisions in these laws and measures are often very general in their wording – the Specification provides a more granular, comprehensive approach to data protection that can ease the confusion created by conflicting standards.

The definition of "personal information"

The Specification broadens the definition of personal information under the 2013 Guidelines and under the Cyber Security Law to include information reflecting not just the factual and biometric attributes, but also the activities of a particular natural person, including an individual's location data, correspondence records, online browsing history, transaction information and so forth.

The Specification follows the logic of the 2013 Guidelines and "distils" sensitive personal information from (more general and hence less sensitive) personal information. "Sensitive personal information" is defined as "personal information which can potentially put personal or property safety at risk, or which is very likely to cause damage to, or discrimination with respect to, an individual's reputation, physical or mental health if disclosed, unlawfully provided or misused". Non-exhaustive examples of sensitive personal information listed in the main body of the Specification include identification card numbers, biometric identification information, bank account numbers, correspondence records, property information, credit information, location data, residential information, health information, transaction information, personal information of minors of 14 years of age or under and so forth. Personal information which has been anonymised will not be treated as personal information.

The Specification includes annexures giving further examples of personal information and sensitive personal information, respectively. Further examples of sensitive personal information include online identity information (such as system account number and email address and passcode, password, answers to security questions relating to the foregoing, and user's personal digital certificates), personal telephone number, sexual orientation, marital history, religion, unpublished records of law violations, website browsing history, and precise positioning information.

GDPR imposes stricter requirements on "special categories of personal data"

Under the GDPR, "special categories of personal data" (broadly similar to "sensitive personal data" under EU Directive 95/46) are regulated more heavily (for instance, a data protection impact assessment on such data will be required under certain circumstances). However, the scope of "special categories of personal data" under the GDPR appears to be narrower than "sensitive personal information" under the Specification. "Special categories of personal data" means personal data processed to reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the

purpose of uniquely identifying a natural person, and data concerning health or data concerning a natural person's sex life or sexual orientation.

The collection and use of personal information

Under the Specification, prior to the collection of personal information, certain disclosures need to be made and/or certain steps need to be taken. Some of these requirements are simply repeating the requirements under the 2013 Guidelines; others are new.

- Collection from data subjects

  A data controller must expressly inform personal information data subjects of each type of personal information to be collected corresponding to each different business function of the product or service in question (explained further below), as well as rules for collecting or using personal information (e.g. the purpose for which the personal information is collected and used; how and how often personal information is collected; where and for how long the personal information is to be stored; its ability to keep data secure; whether such personal information is to be shared, transferred or disclosed). After such disclosure, consent must be obtained from data subjects.

  A data controller must develop privacy policies. In addition to the information in the preceding paragraph, there is other prescribed information that must be disclosed in the privacy policy. A sample privacy policy is included as an appendix in the Specification. Based on our experience, achieving compliance means the typical online privacy policy we have seen being used in the Chinese market will need to be revised quite significantly.

  Under the 2013 Guidelines, there was no mention of a compulsory privacy policy, and no requirement to disclose where the personal information is to be stored.

- Collection from third parties

  A data controller must require the supplier of personal information to indicate the source from which the personal information was originally obtained, and verify the lawfulness of such source; it must also learn about the scope of authority having been granted to the supplier of the personal information for processing the personal information, including the purpose(s) of the use, and whether the personal information subject consents to its transfer, sharing and disclosure. If processing of personal information outside the scope of the authority granted is required, explicit consent from the personal information subject must be obtained within a reasonable period following acquisition of such personal information or prior to processing the personal information.

  The above requirements to ascertain the source of information and verify its lawfulness are new. Although they are likely to increase the costs of personal data collection by companies, they may have the benefit of it minimizing the risk that the data collector will be held criminally liable for violating Article 253 of the *PRC Criminal Law* (revised to take effect from 4 November 2017), which states that any person who unlawfully obtains citizens' personal information by theft or through other means will be held criminally liable.

- Collection of sensitive personal information

> As with the 2013 Guidelines, the collection of sensitive personal information is subject to stricter requirements – an explicit consent must be obtained and such explicit consent must be made by the personal information subject after being fully informed, and on a voluntary basis, and must reflect his/her specific and clear intent. The Specification also requires a data controller to distinguish between "core business functions" and "additional business functions" of the products or services it provides. With respect to sensitive personal information required to be collected for realizing "core business functions" e.g. to register on the network, identify the client and send or receive payment of bills in the case of a mobile telephone operator, a data subject must be given the option to choose whether to supply sensitive personal information or whether to agree to automatic collection, after being explicitly informed of the consequences of refusing to supply the personal information or providing consent (e.g. termination of service). Where a data subject refuses to provide his or her personal information required for the provision of additional business functions e.g. optional services like international data roaming, such additional business functions may be removed, whilst the core business functions must not be terminated on such grounds and the quality of service must not be affected.

A valid form of explicit consent means either: (i) providing a written acknowledgement; or (ii) taking voluntary affirmative actions (such as voluntary acknowledgements made either electronically or physically, voluntary "box checking", voluntary clicks on the "Agree", "Register", "Send" or "Call" buttons and so forth).

The collection of personal information from minors between 14 and 18 is subject to explicit consent from either the minor or his/her legal guardian. The collection of personal information from minors under 14 requires explicit consent from his or her legal guardian.

Consent requirements are in some ways more flexible than the GDPR, but the Standard does not permit "legitimate interests" processing

Localizing data handling processes developed under GDPR compliance programs to China will involve some important changes, consent requirements being a key area to note.

Under the GDPR, silence, pre-ticked boxes or inactivity do not constitute consent. An explicit consent, similar to China, is required to be obtained for not only "special categories of personal data", but also for all types of personal information, unless a derogation is available, for example, the processing is justified by the data controller's legitimate interests.

The legitimate interests derogation is a critical tool for compliance programs under the GDPR, given the strictness of consent requirements.

The collection of personal information under the Standard permits implied consent as a basis for processing. This is likely, in the online context in particular, to ease the burden on lawful collection, even if there is no concept of legitimate interests available to Chinese data controllers. There is also a list of exemptions from the consent requirement that broadly tracks the lists of exemptions found under the GDPR and national data protection laws found in the Asia-Pacific region, including exemptions for processing required by applicable law, for the purpose of investigating criminal activity and as may be necessary for the performance of a contract entered into by the data subject.

This is the first time that China has articulated exceptions to the consent requirement. It is anticipated that the "necessary to perform contract" exception will be the most welcome and widely-used one, and companies will seek to rely on this exception to process significant volumes of personal information.

Importantly, there is also an exception for personal information which has been publicly disclosed by the data subject, which is an important exception in the context of online data processing, such as through social media. There is no corresponding exception under the GDPR, and it will be interesting to see how this exception can be reconciled with the "right to deletion" found in article 7.6 of the Specification, which has been noted by some commentators to be China's equivalent of the GDPR's "right to be forgotten".

Transferring, sharing and (publicly) disclosing personal information

- Required disclosure and consent

  As with the 2013 Guidelines, under the Specification, prior to data sharing, transfer or (public) disclosure, informed consent must be obtained for the transfer, and data controllers must carry out a personal information security impact assessment and adopt effective measures to protect data subjects, based on the results of such assessment. Unlike the 2013 Guidelines, the name, address and contact method for the recipient do not need to be disclosed to the data subject; the Specification only requires the type of data recipient to be disclosed, unless the transfer of sensitive personal information is involved. Again, explicit consent is only required for the sharing or transfer of sensitive personal information, but (publicly) disclosing any type of personal information will require explicit consent.

- Record keeping

  Accurate records of the sharing and transferring of personal information, including the date, scope and purpose of such sharing and transferring, as well as basic information about the data recipients, must be kept and maintained.

  This is a new requirement. There is a similar but more onerous requirement under the GDPR, but under the GDPR, companies with less than 250 employees are not required to keep records unless the data processing is more than occasional or involves sensitive information. No such exemption exists under the Specification, and enterprises doing business in China will find themselves subject to this extra administrative burden which could be costly.

- Transfer in connection with M&A

  The Specification introduces a new requirement where personal data is to be transferred in connection with a merger, acquisition or restructuring ("**M&A**"). In such M&A transactions, the data controller must notify the data subjects of this fact, and its successor should continue to perform the original data controller's responsibilities and obligations. If the purpose of use has changed post-transaction, the successor must obtain a new explicit consent from the data subjects. The requirement to notify data subjects for the data transfer in M&A deals is a new requirement. In the past, we have commonly seen that reliance has been placed on prior consent obtained (via employee handbooks or company

policies) from individuals for the potential transfer of personal data in case of M&A, and no notification of the M&A deal *per se* was required. This new requirement clearly adds an administrative burden on companies in M&A transactions.

- Cross-border transfer

  The Specification does not purport to regulate cross-border personal data transfer, other than to say that the data controller must carry out a security assessment in accordance with the measures and relevant standards prescribed by the CAC in conjunction with relevant departments under the State Council.

  For discussion of cross-border personal data transfers, please refer to our earlier briefing here: *China's Revised Draft Data Localisation Measures*. Although the *Security Assessment for Personal Information and Important Data Transmitted Outside of PRC Measures* ("**Draft Export Review Measures**") issued by the CAC last year was still in draft form at time of writing, it is expected that if the Draft Export Review Measures are adopted in their current form, cross-border transfers of personal information and/or in relation to cross-border transfers of "**important data"** by network operators will require explicit consent from data subjects. It is important to note that the requirement to conduct a security assessment not only on the cross-border transfer of personal information, but also "important data" is expected to be one of the key differences between the Cyber Security Law and the GDPR. This essentially reflects the political dimension that China sees in certain cross-border transfers of information, allowing China to track and potentially prevent transfers overseas of what it considers to be politically sensitive information and information which may be exploited against Chinese national interests through cyber-espionage, a concept closely linked to the nebulous and malleable definition of state secrets. These considerations have no counterparts under the GDPR.

The rights of data subjects

Compared with the 2013 Guidelines, the Specification grants data subjects stronger control over their personal information. It is reassuring to see that to a large extent, such rights mirror those under the GDPR. Articles 7.4 to 7.10 of the Specification confer the following rights on a personal information subject:

- to access personal information (this includes access to personal information, the source of such personal information and purpose for which it is used, and the identities or types of third parties who have obtained such personal information);
- to rectify personal information;
- to erase personal information if the collection, use, share, transfer or public disclosure of the personal information are in violation of laws or regulations, or agreements;
- to withdraw consent including the right to refuse to receive commercial advertisements;
- to deregister accounts;
- to obtain copies of certain types of personal information, or transfer the same directly to a third party; or

- to lodge complaints where decisions which significantly affect the rights and interests of personal information subjects are made solely on the basis of automatic decision-making by the information system.

With respect to the right to copy and the right to data portability, the right is limited to basic personal information, personal identity information, personal health and physiological information, education and employment information ("**Restrictions**"). The rationale behind the Restrictions is not clear, as portability generally enhances consumer protection, but may be the result of lobbying by industry players who see this as a cost issue. Such Restrictions do not exist under the GDPR.

Despite giving data subjects the above-mentioned rights, the Specification specifies certain circumstances under which the data controller may choose not to respond to requests by personal information subjects.

The Specification gives the data controller 30 days to respond to requests from data subjects. Under the GDPR, it is generally one month, but the response can be postponed for up to two months, taking into account the complexity of the request and the large number of requests.

Other key requirements under the Specification

Other key requirements under the Specification which were not in the 2013 Guidelines include:

- One of the critical questions for compliance under the GDPR is whether or not the organization is required to appoint a data protection officer ("**DPO**"), an individual charged with responsibility for monitoring and advising on GDPR compliance. The Specification has no specific analogue to the DPO requirement, but it is notable that data controllers are required to appoint a head of personal information protection and, in cases of organizations employing more than 200 individuals or processing the personal information of more than 500,000 individuals, this individual is required to be dedicated to this role;
- With respect to data storage, data controllers are recommended to de-identify personal information as soon as it is collected and implement technical measures and controls to keep de-identified data separate from information that may be used to re-identify the individual in question in order to ensure that the individual will not be re-identified during any subsequent processing of the personal information; adopting security measures, such as encryption, in the course of transmitting and storing sensitive personal information. This requirement is not explicitly replicated under the GDPR, although in practice re-identification risk must be managed using these and other techniques in order to avoid unlawful processing of re-identified personal data;
- With respect to the use of personal information, certain internal controls for accessing personal information should be in place, such as access limitation and minimization, internal approval process for important operations, and access records keeping; certain limitations must be put on the use of personal information, such as limiting the use of personal information to the effect that the information is not linked to a specific individual, except to the extent necessary to achieve the purposes of collection and use. For example, direct user profiling may be used to obtain an accurate assessment of an individual's credit

standing, whilst indirect user profiling is preferred when the personal information is being used to send commercial advertising;

- When using an agent to process personal information, the data controller must ensure that (i) the engagement must not go beyond the scope of consent obtained, or go outside the exceptions to requirement for consent; (ii) carry out a personal information security impact assessment on the engagement to ensure the agent has sufficient data protection capabilities in place to provide the required level of protection; (iii) supervise the agent by means such as defining the agent's duties and obligations in a contract or otherwise, or carrying out an audit; and (iv) maintain accurate records of processing activities carried out by the agent;
- With respect to the handling of security incidents involving personal information, data controllers are required to (i) formulate contingency plan for security incidents involving personal information and update the plans when necessary; (ii) conduct internal training and emergency drills at least once a year; (iii) in the event of a security incident, recording the facts about the incident, including but not limited to: the person who identified the incident; the time and place at which the incident was identified; the personal information and number of individuals involved; the name of the system in which the incident occurred; the impact on other interconnected systems; whether law enforcement or relevant authorities have been contacted, adopt necessary measures to contain the situation and eliminate hidden dangers, and report the incident to the relevant Chinese authorities; and (iv) inform the affected data subjects;
- Appointing a personal information protection officer and personal information protection working group. For certain organizations (core activities involving processing personal data with over 200 staff, or processing personal data involving over 500,000 individuals, or expected to do so within the next 12 months), such officer and working group must be dedicated to work on personal information protection; and
- Implementing a personal information security impact assessment system to carry out personal information security impact assessments as required under the Specification and at least once a year.

How to approach to data protection compliance in China?

It is perhaps no coincidence that the Specification was given effect in May, 2018, the same month that saw the implementation of the GDPR. It is clear that the Specification takes much in the way of inspiration from the GDPR, the instrument recognized as the leading edge of regulatory innovation in data protection globally, and represents a concerted push by China towards more responsible and accountable use of personal information.

The Specification is the most definitive and substantial statement of recommended practice in relation to data protection issued by China to date. The fact that it is not law in the formal sense muddies the waters a little in terms of legal enforceability and consequences for non-compliance. Initial signs are that the Specification is being treated as 'quasi-law' by the CAC, and that the standards laid down in it are being used to hold the feet of certain business operators to the fire, which in a market like China, where players are heavily dependent on government support for maintaining licenses, comes pretty close to having the same practical effect as law enforcement.

It is also important to note that in addition to the Cyber Security Law, laws such as the Consumer Protection Law impose general data protection obligations which can be well served by taking the more granular approach set out in the Specification as the practical working standard for compliance.

For organizations that have already invested in GDPR compliance programs, the themes of compliance with the Specification will be familiar. The Specification represents comprehensive data protection compliance that is best served by a compliance strategy similar to that deployed in relation to the GDPR:

- **Project management discipline**: Like GDPR compliance, compliance with the Specification requires a multi-disciplinary approach, drawing on information inputs and decision-making by personnel from functional areas such as marketing, information technology, operations management and human resources, in addition to the efforts needed from legal and compliance staff,
- **Information is critical**: Organizations that have completed GDPR implementation programs will be well-versed in data inventory programs which seek to map out the organization's various holdings of personal data and understand how this data was collected, for what purposes it is being processed and to whom it is being transferred. This first step is critical to any compliance assessment.
- **Compliance in fact**: Once armed with reliable information about the organization's personal information holdings, a compliance assessment can be made and the organization can move towards developing a compliance program that meets the applicable requirements (both in respect of the Specification and applicable industry-specific data protection laws). The policy documentation typically seen in a GDPR implementation program will likely outweigh a corresponding set of policy documents for China, but we see benefit to adopting a common general structure that ensures that the China program effectively interfaces, as appropriate, with the global program.
- **Prioritization, prioritization, prioritization**: As with GDPR compliance programs, there is a risk of being overwhelmed by the volume of factual information and requirements that need to be met. Sensible prioritization is recommended, focusing on areas that are more likely to generate complaints and give rise to the risk of loss of sensitive personal information. Some key actions that will need to be taken include:
- Reviewing and updating data protection consents and notifications;
- Developing and implementing an internal policy concerning personal information collection, processing and transfer;
- Devising internal controls for accessing personal information, such as access limitation and minimization, internal approval processes for important operations, and record-keeping of access;
- Reviewing current use of personal information to ascertain whether certain limitations should be put on such use;
- Ensuring internal procedures are put in place or updated to cover all the rights data subjects are entitled to, including data erasure and data portability;

- Implementing measures to keep accurate records of the sharing and transferring of personal information;
- Checking to see whether sensitive personal information is being collected and if so, ensure stricter controls are in place, such as applying encryption to the data transfer, adopting mechanisms to obtain explicit consent for collection, use or transfer;
- If third party data processors are used to process personal information, complying with the requirements under the Specification (discussed above), especially by conducting a personal information security impact assessment and making sure a robust contract is in place;
- If automatic decision-making by information system is involved, providing personal information subjects with a way to contest the decision;
- If personal information is being collected from third parties, ensuring each source of personal data is lawful and consent has been obtained for the data sharing/transfer;
- Implementing a personal information security impact assessment system to carry out personal information security impact assessments where required under the Specification;
- Formulating a contingency plan for security incidents that involve personal information and conduct emergency drills at least once a year; and
- Having adequate systems in place to verify data subjects' ages and collect consent from guardians if required.

Contacts:

Andrew McGinty
Partner, Shanghai
andrew.mcGinty@hoganlovells.com

Mark Parsons
Partner, Hong Kong
mark.parsons@hoganlovells.com

Jun Wei
Partner, Beijing
jun.wei@hoganlovells.com

Roy Zou
Partner, Beijing
roy.zou@hoganlovells.com

Sherry Gong
Counsel, Beijing
sherry.gong@hoganlovells.com

Jessie Xie
Senior associate, Beijing
jessie.xie@hoganlovells.com

Maggie Shen
Senior associate, Shanghai
maggie.shen@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices

www.hoganlovells.com