Bloomberg BNA

Privacy and Security Law Report®

Privacy Changes Coming to China




BY MIRIAM H. WUGMEISTER, PAUL D. MCKENZIE, GABRIEL BLOCH, AND JINGXIAO FANG

There is continued focus in China on privacy and data security issues. China still has no omnibus law, but it has promulgated some sector-specific regulations.[1] The latest of these regulations governs protection of consumer data by credit reporting agencies. More significantly, China has issued new voluntary guidelines on management of computerized information of individuals. We discuss both of these developments below.

Voluntary Guidelines

The *Information Security Guidelines for Protection of Personal Information Within Information Systems for Public and Commercial Services* (the "**Guidelines**") took effect Feb. 1.[2] The Guidelines, which were issued as a "national standard" under China's GB ("**guobiao**") standardization system, are not mandatory and thus lack the force of law. That said, we anticipate that the Guidelines will serve as an important reference for companies seeking to develop best practices in order to comply with existing People's Republic of China (PRC) legal provisions that pertain to data privacy, such as the general right to privacy under the Tort Liability Law and the sector-specific regulations mentioned above. Moreover, the Guidelines may serve as an indication of the direction in which the PRC government may be heading with respect to data protection laws in the future.[3]

The Guidelines encompass the full range of obligations found under most omnibus data protection laws and encompass all of the Fair Information Principles as well as some additional obligations. We summarize the Guidelines below.

Key Definitions

- "Personal information" governed by the Guidelines is defined as including any information that: (i) is able to be processed by a computer system; (ii) relates to a specified individual person; and (iii) by itself or in combination with other information could disclose the identity of the individual. As drafted, the Guidelines do not apply to offline data, but there is no description or detail on what it means for data to be "computerized." So, for example, it is not clear if data collected on paper and then scanned into a database would be considered computerized data. Nor is it clear if documents printed out from a computerized database would also be covered.
- The Guidelines distinguish between "general personal information" and "sensitive personal information." Sensitive personal information includes, but is not limited to, an individual's identification

[1] *See* Morrison & Foerster LLP, Client Alert, "China's Legislature Weighs in on Online Data Privacy; Other Recent Privacy Developments in China" (Jan. 23, 2013), *available at* http://www.mofo.com/files/Uploads/Images/130122-China-Privacy-Developments.pdf.

[2] To obtain a copy of an unofficial English translation of the Guidelines please send your request to pmckenzie@mofo.com.

The authors are members of Morrison & Foerster LLP's Global Privacy and Data Security practice.

[3] Draft guidelines were issued for public comment in 2011. The Guidelines as now published adopted a much different structure than that previous draft.

 ISSN 1538-3423

card number, cellphone number, ethnicity, political views, religion, genetic information, and fingerprints. Each sector or industry may add additional data elements to the definition of sensitive personal information.

Notice

Organizations should provide notice to individuals before personal information is collected. The notice should include the following:

- what personal information will be collected;
- the purpose for which the personal information will be used;
- the method of collecting the personal information;
- the retention period of the personal information;
- the party or parties to whom the personal information will be disclosed (including the name, address, and contact details of the recipient of the personal information);
- security measures in place;
- the name and address of a person responsible for the personal information;
- the consequences if the individual elects not to provide the personal information;
- a complaint mechanism; and
- the ''possible risks'' of providing the personal information.

Choice

Organizations should provide a choice to individuals with regard to the collection, use and transfer or their personal information. An individual's prior express consent (i.e., opt-in) should be obtained when collecting sensitive personal information. For general personal information, tacit or opt-out consent should be requested. Any subsequent requests to cease the processing of personal information should be honored.

Access/Correction/Deletion

The Guidelines contemplate that individuals should be able to request access to and correction of personal information. In addition, if an individual requests deletion of his/her personal information on ''justifiable grounds,'' the organization should delete it ''promptly.''

Security/Audits

As in most data protection laws, the Guidelines provide that organizations should take appropriate management and technical measures to protect personal information from serious damage and to protect it from being ''retrieved, divulged, lost, disclosed, damaged or altered without authorization.'' Interestingly, the Guidelines also suggest that organizations should conduct self-audits or engage a third party to evaluate and test their security procedures.

Cross-Border Limitation

The Guidelines include a cross-border limitation and suggest that personal information should not be provided to any organization outside the PRC unless the individual provides opt-in consent, the transfer is required by law, or government authorities authorize the transfer. It is not clear if ''required by law'' refers to PRC law or the law of any other country. The cross-border limitation also does not include any of the other exceptions we typically see in omnibus data protection law such as contractual necessity or for the defense of a legal claim.

Breach Notification

The Guidelines suggest that if personal information has been divulged, lost, or altered, organizations should remediate, provide notice to individuals, and if it is a material incident, promptly notify the appropriate ''personal information protection administration authority.'' The trigger for breach notification is consistent with that found in most data protection laws. The notification requirement is not triggered when there is an unauthorized access or acquisition, but is triggered if the personal information is simply lost or altered. Unlike other breach notification laws which focus on security incidents involving sensitive personal information or information that can result in identity theft or financial fraud, the Guidelines require breach notification if *any* personal information is affected. It is interesting to note that the Guidelines refer to a ''personal information protection administrative authority'' but do not indicate who that is or will be.

Other Interesting Provisions

There are several other interesting provisions in the Guidelines including the following:

- **Children:** No information from an individual under the age of 16 should be collected without parental consent.
- **Data Minimization:** Organizations should minimize the amount of information they collect, use, or retain to the minimum amount possible. As soon as the purpose for which information was collected has been achieved, personal information should be deleted.
- **Data Protection Officer:** An organization should appoint an individual responsible for: ensuring that personal information is properly processed; handling access and correction requests; responding to complaints; ensuring that training is provided; and supervising internal audits.
- **Third Party Testing:** The Guidelines introduce the concept of a ''third party testing and evaluation agency,'' which has the responsibility to supervise protection of personal information and test the security of related computer information systems.

It is anticipated that the Guidelines will be adopted as standards of service in outsourcing and other transactions in China. It is also possible that the Guidelines are a precursor to a law. They may also be used by plaintiffs or enforcement authorities to determine if a company has properly handled personal information. For companies operating in China, it may be wise to carefully review the Guidelines and work with trade associations to provide feedback about the provisions that work and those that are problematic.

Credit Reporting Regulations

On Dec. 26, 2012, the *Credit Reporting Regulations* (the ''**Regulations**'') were approved by the 228th gen-

   ISSN 1538-3423

eral meeting of the State Council, China's cabinet-level body.[4] The Regulations, which will become effective March 15, govern the establishment, operation, and administration of credit reporting agencies (the ''**CRAs**''). Although they are not limited in scope to data privacy issues, the Regulations impose a number of obligations upon CRAs and other entities with regard to their collection and use of personal information in the course of their business operations. We summarize relevant provisions below.

- The Regulations prohibit CRAs from collecting certain types of personal information, such as information relating to religious beliefs, genetic information, fingerprints, blood types, and medical history. They also enumerate certain types of information that CRAs may collect (subject to complying with certain requirements), such as personal information concerning income, deposits, securities, commercial insurance, real estate, and tax payments.
- Prior to collecting certain types of personal information concerning income, deposits, securities, commercial insurance, real estate, and tax payments of an individual, CRAs must obtain the individual's prior written consent and expressly inform such individual of the possible adverse consequences of the disclosure.
- An entity receiving personal information from CRAs must generally obtain the individual's prior written consent and use such information only for purposes agreed upon between such entity and the individual.
- An information provider must inform the individual in advance when disclosing personal information to CRAs that may have adverse consequences on an individual's credit rating. CRAs may only retain such information for five years starting from the date when the related event took place. At the end of the five years, CRAs must delete such information.
- The individual has the right to review his/her personal information collected by a CRA, and to require correction of any errors.
- CRAs must comply with ''relevant regulations'' when providing personal information to offshore entities or individuals. However, we are not aware of any regulations currently in place addressing disclosure of personal information to offshore entities or individuals, although we anticipate such regulations may be promulgated in future.

The Regulations generally provide that competent authorities shall have the authority to take enforcement actions against CRAs violating the Regulations, such as ordering remedial measures, issuing fines, confiscating illegal gains, and revoking licenses.

[4] The *Credit Reporting Regulations* are available, in Chinese, at http://www.gov.cn/zwgk/2013-01/29/content_2322231.htm.