

CY Japan Legal Update

December 2016

Consumer Data Privacy

The Amendment to the Act on the Protection of Personal Information will come into force on May 30, 2017 (Part 1)

Yasuyuki Kuribayashi / Naoki Matsuo

Act on the Protection of Personal Information (the “Law”) was amended and, together with the amendment of the Order for Enforcement of the Act on the Protection of Personal Information (the “Cabinet Order”), it will come into force on May 30, 2017. In the amended laws (the “Amended Laws”), (1) definition of personal information was clarified and several concepts were introduced to strengthen regulations and establish new regulations, and (2) amendments were made concerning the handling, storage and distribution of personal information to deter the unauthorized use of personal information and in response to globalization of data flows. In this article, (1) of those amendments will be introduced.

1. Clarification of definition of personal information

Along with the development of information and communication technology, the Amended Law has put into law that information including individual identification codes will constitute “personal information” as the previous definition of personal information (determining identifying with reference to other information) was vague and to clarify the scope of personal information for both business operators and consumers. “Individual identification codes” means codes determined by the Cabinet Order by which a specific individual may be identified of (1) codes which convert physical characteristics of a specific individual for the use of electronic computers or (2) codes assigned variably for each individual described or recorded in documents or electronic computers.

The Amended Cabinet Order provides as specific examples of (1): DNA sequence data, facial recognition data, iris pattern data, voiceprint data, gait pattern data, palm/finger vein pattern data and fingerprint/palmprint data and as specific examples of (2): passport number, basic pension number, driver’s license number, individual number (so-called “My Number”) and national health insurance number. Under the Amended Cabinet Order, the Rules of the Personal Information Protection Commission can further designate individual identification codes in addition to such individual identification codes.

2. Regulations concerning Sensitive Personal Information

The Amended Law introduced the concept of “sensitive personal information” to establish special laws the same as laws in countries including the EU and to categorize personal information which may be the cause of social discrimination.

“Sensitive personal information” means personal information which contains the descriptions specified by Cabinet Order to require special consideration in handling in order to avoid any unfair discrimination, prejudice or other disadvantage to an individual, including race, creed, social status, medical history, and criminal record.

The Amended Law provides as regulations for sensitive personal information, first, business operator handling personal information must obtain the consent of the subject person in advance in principle to obtain sensitive personal information, second, in regard to sensitive personal information, third party provision through opt-out procedures (a structure of being able to provide to a third party without the prior consent of the subject person on the condition of (i) if requested by the subject person, suspension of third party provision, and (ii) prior notification to the subject person the items of personal information to be provided and provision method, etc. or have in place a situation where the subject person can easily know) is not permitted.

3. Regulations concerning De-identified Information

The Amended Law has introduced the concepts of de-identified information and business operator handling de-identified information to ensure the protection of personal information and to promote the use of enormous personal data collected through the development of ICT (information and communication technology).

“De-identified information” means information which is processed so that it cannot identify a specific individual by taking prescribed measures and information for which such personal information cannot be restored. Specifically, it is anticipated to be big data information where while information which may identify an individual is deleted, other raw data is maintained. De-identified information is not affected by restrictions for the purpose of use of original personal information and with the purpose of using beyond the purpose of use regarding the original personal information, it is permitted to produce the de-identified information by processing such information.

“Business operator handling de-identified information” means a person providing a database in which specific de-identified information may be easily searched for business purposes. “Business operator handling de-identified information” may provide de-identified information to a third party without obtaining consent from the subject person of the personal information used for such preparation if the items of such information and provision method is made public and (ii) such information being de-identified information is indicated to the provision counterparty for de-identified information. Even in the case of handling of “de-identified information” beyond the scope of purpose of use in the original personal information used in the preparation of the de-identified information, no particular obligation to obtain the consent from the subject person of the personal information used in such preparation or obligation to give notice, etc. to the subject person before or after is imposed.

Such standards and methods are provided for in the Rules of the Personal Information Protection Commission in regard to the preparation, management provision, and publication and other such matter for de-identified information.

4. Responses required of business operators

After the enforcement of the Amended Law, under the above 1 and 2, business operators, who did not handle information including individual identification codes as personal information, are required to handle such information the same as other personal information in the future and must obtain the consent of the subject person in the case newly acquire information is sensitive personal information or in the case of provision to third parties after enforcement even for information acquired before the enforcement. As well, business operators who conduct business which utilized de-identified information must comply with the standards of the Rules of the Personal Information Protection Commission in the preparation and use of de-identified information.

For more information, please contact:

Yasuyuki Kuribayashi, Partner
yasuyuki.kuribayashi@city-yuwa.com