Guidelines for Protection of Big Data Personal Information

On December 23, 2014, the Korea Communications Commission announced the 'Guidelines for Protection of Big Data Personal Information' detailing specific standards for the protection and safe use of personal information in connection with the processing and utilization of big data.

1. First guidelines relating to Big Data

Big Data is defined as a large volume of information including real-time, unstructured data, and is becoming recognized as an economic asset to create new added values. There are increasing calls for the promotion of the big data industry as part of the nation's industrial policy. However, in addition to the growth of big data processing technologies, due to the advancement of profiling technologies such as the ability to predict the propensities and behaviors of users through data analysis and the making of unidentifiable information identifiable through combination and analysis of such unidentifiable information, there is also an increasing concern about privacy invasion.

The current personal information protection laws, including the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc., require prior consent of the users via the so-called "opt-in" method before collecting or using personal information. However, given the nature of big data and the difficulties in obtaining prior consent to collection and handling of such data given the sheer volume, the requirement to obtain prior consent has stymied developments without, in practice, satisfying the objective of providing protection with respect to the personal information. For this reason, the opt-in based approach has turned out to be ineffective in protecting users' personal information, leaving business operators discontent with regulatory uncertainties.

To address these issues, the Guidelines propose measures to prevent business operators (i.e., information and communication service providers) from abusing or misusing users' personal information by creating new information by collecting, storing, combining and analyzing "publicly

available personal information" or details of the history of access or use automatically generated when users have accessed or used such information and communication services, and to maximize the utilization of big data under the related laws and regulations.

2. Strict measures relating to de-identification (Sections 3, 4, 5, etc.)

If publicly available information or details of access history contain personal information, the Guidelines require business operators to delete or replace all or part of such personal information from and at the stage of data collection through deletion, pseudonymisation, aggregation, categorization and data masking, thereby making impossible to identify a particular user, even if such personal information is combined with other information. Further, business operators who have taken these measures are allowed to collect and exploit personal information without user's consent (Article 4), provide such information to a third party (Article 10), and use them internally for the purpose of provision of their services, unless the user expressly refuses (Article 9). This is the most important aspect to the Guidelines to balance the protection of users' personal information and the utilization of big data by business operators.

3. Promotion of transparency (Sections 4, 5 and 6)

Due to advancement in information technology, users are exposed to an ever-present danger of privacy invasion and their personal information is likely to be collected and exploited even without their knowledge. To remedy this situation, the Guidelines require business operators to disclose (i) the fact that they are collecting and using publicly available personal information and details of access history containing personal information; (ii) the source and the purpose of collecting personal information; (iii) the fact that new information containing users' personal information may be generated from the data collection process; and (iv) the method of handling such new information. In respect of the collecting and handling of publicly available personal information, the Guidelines also require business operators to notify their users that they are entitled to request disclosure of the source and the purpose of such collecting and handling of such information, as well as suspension of handling of such personal information.

4. Immediate destruction of re-identified personal information and measures to make such personal information unidentifiable (Sections 3 and 6)

If any information generated after processing publicly available personal information or the details of access history made unidentifiable, contains identifiable personal information, business operators are required to immediately destroy such information or take additional measures to make it unidentifiable.

5. Prohibition on collection, exploitation or analysis of sensitive information and communications secrets (Sections 7 and 8)

Unless otherwise agreed by the relevant user, the processing of, data designed to generate sensitive information, including a particular individual's ideology, beliefs, or political opinion, or, the contents of communications such as emails being transmitted or text messages is prohibited.

6. Technical, managerial measures to protect collected information for storage and maintenance (Section 3(2))

Business operators should take protective measures, in technical and managerial terms, with respect to the data processing system that stores and manages information to ensure such information is unidentifiable. In particular, business operators should establish an access control system to prevent infiltration, take measures to prevent forgery of access records, and install and operate antivirus software to avert infiltration by malicious programs.

7. Conclusion

The Guidelines are significant in that they set out a reasonable standard to seek balance between the protection of personal information and the growth of the big data industry under the current laws and regulations for protection of personal information. The Guidelines are expected to be a meaningful starting point to promote the big data industry, a new growth engine in the area of the Internet, while also affording protection of personal information. It is advisable that business operators should streamline their business process to comply with the standards set forth in the Guidelines and should take proper technical, managerial protective measures with respect to information to be stored and maintained.

Should you have any questions regarding any of the foregoing, please feel free to contact us at any time.

- Jongsoo Yoon(Partner) TEL : 02 316 4040 E-Mail: jsyoon@shinkim.com
- Michael Chang(Partner) TEL : 02 316 4653 E-Mail: mchang@shinkim.com

Chambers Asia-Pacific Awards 2014
South Korea Law Firm of the Year : Shin & Kim