LEGAL UPDATE | KOREA

bkl BAE, KIM & LEE LLC

September 22, 2016

BKL Data Privacy Legal Update

Kwang Jun KIM
T 82.2.3404.0481
E kwangJun.kim@bkl.co.kr

Kwang Hyun RYOO
T 82.2.3404.0150
E kh.ryoo@bkl.co.kr

Tae Uk KANG
T 82.2.3404.0485
E taeuk.kang@bkl.co.kr

Susan PARK
T 82.2.3404.0274
E susan.park@bkl.co.kr

1. Proposed Amendment to the Enforcement Decree of PIPA

Following the amendments to the Personal Information Protection Act ("PIPA") which took effect on March 29, 2016, the draft of the amendment to the Enforcement Decree was published for comment by the Ministry of Interior ("MOI", formerly known as the Ministry of Government Administration and Home Affairs) on May 9, 2016. The draft Enforcement Decree provides the specifics of the newly amended PIPA. Key terms of the draft are summarized below.

1) Notification Requirement for Third-Party Transfers

Under the newly amended PIPA, when processing personal information acquired indirectly by way of a third-party transfer, transferees who meet certain threshold prescribed in the Enforcement Decree must notify the data subject of (i) the third party source (transferor) from which the personal information was acquired and (ii) the intended use of the obtained personal information, etc.

Prior to the latest amendments to the PIPA, it was sufficient for the transferor to have obtained valid consent from the data subject with respect to any third-party transfer, and transferees were required to notify the data subject of the occurrence of such-third party transfer only when inquired by the data subject. Effective as of September 30, 2016, however, all third-party transfers received by transferees that meet the threshold under the Enforcement Decree will be subject to such notification.

The current draft of the Enforcement Decree proposes that the obligation to notify the data subjects in case of receipt of personal information from a third party be imposed on:

(a) anyone who processes 'sensitive information' or 'unique identifying information' of 50,000 data subjects or more; or
(b) anyone who processes personal information of 1 million data subjects or more.

* *Sensitive information* is defined in the PIPA as information regarding whether one has joined or withdrawn from a labor union or political party, political opinions, health, sexual life, genetic data and criminal record.

* *Unique identifying information* refers to the Resident Registration Number (RRN), driver's license number, passport number or foreign resident registration number.

Further details on how and when the notification should be given are also provided in the draft Enforcement Decree. According to the draft, the notification must be in writing, by phone, by text message, or e-mail, etc. and be made within three (3) months from the date of receipt of the personal data from the transferor. In addition, the transferee must keep record of the fact that the notification was made (including the date and method of notification) until the relevant personal information is destroyed.

Thus, effective as of September 30, 2016, companies that either process sensitive information or unique identifying information of 50,000 data subjects or more, or process personal information of 1 million data subjects or more should be prepared to implement the obligation to notify data subjects if personal information has been obtained indirectly from third parties.

2) Obligation to Submit to Regular Inspection by MOI

A new provision has been added to the PIPA authorizing the MOI to conduct periodic inspections on certain data processors (as defined by the Enforcement Decree) to ensure that the requisite security measures are properly implemented. This provision will likewise come into effect on September 30, 2016.

Under the current draft of the Enforcement Decree, such regular inspections must be conducted at least once every two years on (a) public institutions, (b) those handling unique identifying information of 50,000 data subjects or more, and (c) those who handle personal information of 1 million data subjects or more. The inspection shall be conducted by way of document review; however, the inspection may be expanded to site inspection if (i) the data processor fails to submit documents requested by the MOI, (ii) a violation of the obligation to maintain security measures is discovered or suspected, or (iii) any complaint from the data subject regarding the same is lodged.

Thus, effective as of September 30, 2016, companies that process either unique identifying information of 50,000 data subjects or more, or personal information of 1 million data subjects or more, should be prepared to comply with MOI's request for document review in connection with MOI's regular inspection on the company's security measures.

2. Proposed Amendment to the Enforcement Decree of the IT Network Act

On July 7, 2016, the Korea Communications Commission ("KCC") announced its proposal to amend the Enforcement Decree of the Act on the Promotion of IT Network Use and Information Protection ("IT Network Act"), which is the data privacy law pertaining specifically to IT service providers including online businesses as well as telecommunications companies.

1) Clarification of Statutory Retention Period Applicable to Unused Data

The proposed amendment addresses, among other things, the issue of how the IT service providers should handle personal data whose "statutory retention period" has expired, but which data the IT service provider has a legal obligation to retain pursuant to other laws.

Under the IT Network Act, IT service providers are required to destroy or separately store "expired" personal information which has not been used by the IT service providers for more than 1 year, which is the statutory retention period. However, it was not clear whether the 1-year statutory retention period applied to personal information which was required to be retained for a longer term under other laws (e.g., e-commerce transaction records of consumers, which must be kept for 5 years pursuant to the E-commerce Act).

The current draft of the Enforcement Decree serves to clarify this point, by expressly requiring that such personal information that are required to be kept by law for a longer period be kept separately from other 'active' personal information once the statutory retention period expires.

Accordingly, IT service providers would be required to separately store such personal information once the 1-year period expires.

In connection with the '1-year statutory retention period', the KCC recently imposed administrative fines on a major online business operator which failed to comply with the destruction or separate storage obligation of such 'expired' personal information.

On August 11, 2016, the KCC announced that (i) seven IT service providers, including CJ O Shopping, GS Homeshopping and Hyundai Homeshopping, were imposed corrective orders and a fine in the range of 5 million to 10 million Korean Won for failure to destroy or separately store such 'expired' personal information, and (ii) ten IT service providers were imposed corrective orders and a fine in the range of 10 million to 15 million Korean Won for failure to take the security measures as required by the IT Network Act, such as encryption of personal information.

3. Upcoming Important Dates

Some important dates relating to data privacy are outlined below.

- November 28, 2016: Sending of reminders to data subjects who have agreed to receive advertisement information.

Effective as of November 29, 2016, under the IT Network Act, advertisement-related information transmitted electronically will be regulated more rigorously to prevent unwanted SPAM. As part of the regulation on SPAM, data processors will be required to send reminders, once every two years, to those data subjects who have previously agreed to receive advertisement information. This means that by November 28, 2016, data processors must send reminders to those who gave consent prior to November 29, 2014.

The reminder must contain the following information:

i) Name of the data processor sending the advertisement-related information;
ii) The fact that the data subject gave consent to receiving advertisement-related information and the date of consent; and
iii) Method to maintain or withdraw consent

It is to be noted that this reminder does not mean that the data processor needs to re-obtain the data subject's consent, and a simple reminder containing the above-listed items will suffice. No response from the data subject is required to fulfill this obligation.

This requirement does not apply to 'expired' personal information which has been separately stored pursuant to the 1-year statutory retention period.

Failure to provide such reminder every two years may result in an administrative fine of up to 30 million Korean Won.

- January 1, 2017: Encryption of Resident Registration Numbers

As a heightened security measure regarding Resident Registration Numbers ("RRNs"), all RRNs must be encrypted. This security measure is being introduced gradually: Data processors holding fewer than 1 million RRNs must complete the encryption of RRNs by January 1, 2017, whereas data processors holding 1 million RRNs or more must complete the encryption by January 1, 2018.

- Less than 1 million RRNs: Encryption must be completed by January 1, 2017
- 1 million RRNs or more: Encryption must be completed by January 1, 2018

4. Alert to Foreign-Invested Companies / Multinationals

Pursuant to the amended IT Network Act, the penalty provisions on overseas transfer of personal information will come into force as of September 23, 2016. Thus, it would be advisable for companies that share databases with its global headquarters and affiliates located outside Korea to ensure that they are in compliance with the IT Network Act in regard to overseas transfer.

The newly introduced penalties are as follows:

- Failure to obtain consent where the overseas transfer of personal information was subject to consent: Administrative penalty in the amount of 3% of the revenue generated in connection with the breach.

- Failure to notify or disclose the overseas transfer of personal information, where such transfer was subject to notification or disclosure: Fine of up to 20 million Korean Won.