LEGAL UPDATE | KOREA

bkl BAE, KIM & LEE LLC

April 26, 2016

2016 Spring Data Protection and Privacy News Alert

The Personal Information Protection Act underwent amendments on July 25, 2015 and on March 2, 2016, followed by the amendment to the Act on the Promotion of IT Network Use and Information Protection on March 22, 2016. These amendments reflect the general trend concerning the Korean data privacy policy, which is intended to achieve more stringent regulation (and sanctions) of processing of personal information and the alignment of the two laws in certain respects.

Recent Amendments in the Personal Information Protection Act ("PIPA")

1. Introduction of Notification Requirement for Third Party Transfers

When processing personal information acquired indirectly by way of a third party transfer, transferees who meet a certain threshold as provided by the Presidential Decree (yet to be announced) will be obligated to 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 received personal information, etc.

Prior to the amendment, it was sufficient for the transferor to have obtained valid consent from the data subject with respect to the third party transfer, and transferees were only obligated to notify the data subject of the occurrence of such third party transfer when inquired by the data subject. Effective as of September 30, 2016, all third party transfers received by transferees who meet the threshold under the Presidential Decree will be subject to such notification.

Tae Uk KANG
T 02.3404.0485
E taeuk.kang@bkl.co.kr

2. Security Measures for Sensitive Information

As amended, the PIPA requires that the same technical, managerial and physical security measures, as required under the PIPA for personal information, be undertaken for sensitive information. This provision will come into effect on September 30, 2016.

3. Types of Government Regulation Authorizing Processing of Resident Registration Numbers

Resident Registration Numbers ("RRNs"), unlike other types of personal information, can only be processed if statutes or subordinate regulations specifically authorize or require such processing, irrespective of the data subject's consent. Effective as of March 30, 2017, the subordinate regulations which can serve as the legal grounds for processing RRNs will be limited to the following regulations: Presidential decrees, National Assembly regulations, Supreme Court regulations, Constitutional Court regulations, National Election Commission regulations and Board of Audit and Inspection regulations. Regulations issued by other government agencies will not constitute as valid legal grounds for processing of the RRNs.

4. Introduction of Statutory Damages and Punitive Damages

Effective as of July 25, 2016, victims of personal information loss, theft, leak, falsification, alternation or damage caused by willful misconduct or gross negligence of the data processor may claim civil damages in the amount of up to KRW 3 million without having to prove actual damages. In addition, victims will be able to claim punitive damages, in the amount not exceeding three times the amount of actual damages.

5. Regular Inspection on Encryption of RRNs

As a heightened security measure regarding RRNs, all RRNs must be encrypted. This security measure is being introduced gradually: Data processors holding less 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.

Furthermore, a new provision has been added to the PIPA which authorizes the Ministry of Interior (formerly Ministry of Government Administration and Home Affairs) to conduct periodic inspections to ensure compliance with the RRN encryption requirement. This provision will come into effect on September 30, 2016.

Key Amendments to the Act on the Promotion of IT Network Use and Information Protection ("IT Network Act")

Set forth below are key changes pursuant to the amendment to the IT Network Act which was announced on March 22, 2016. Unless otherwise specified below, the amended IT Network Act will come into force six months after the date of announcement or September 22, 2016. Further details of the amendment will be supplemented by the presidential decree of the IT Network Act to be amended in due course.

1. Reinforced Consent Requirement for Access to Smartphones (effective as of March 22, 2017; one year from the announcement date)

Smartphone application developers who need access to the data stored in smartphones and to the functions installed in smartphones shall: (i) notify the smartphone users by distinguishing functions which require mandatory access (which are necessary for the operation of the principal function of the program) with functions with optional access and (ii) obtain consent thereto.

2. Improvement to the Regulation of Entrustment Relationships

In case of an entrustment of processing of personal information, the entrustor must 'train' as well as manage the entrustees. Entrustment agreements shall be executed in writing and re-entrustment shall only be permitted upon entrustor's approval. The main purpose of this amendment is to align the respective provisions of the IT Network Act with those of the PIPA.

3. Strengthened Responsibilities of CPO

In case CPO becomes aware of any violation of the data privacy laws, the CPO shall immediately take remedial measures and, where necessary, report such violation to the CEO. The legislative intent of the proposed amendment is alignment with the PIPA.

4. Introduction of Punitive Damages (effective as of July 25, 2016)

Victims of personal information loss, theft, leak, falsification, alternation or damage caused by willful misconduct or gross negligence of the processor will be able to claim punitive damages, in the amount not exceeding three times the amount of actual damages. (Note: The legislative intent of this amendment is to align with the corresponding provisions of the PIPA.)

5. Confiscation and Forfeiture in case of Personal Information-related Crimes

Similarly, any financial gains illegally gained from criminal activities involving personal data shall be subject to confiscation or forfeiture by the government. The legislative intent is also the alignment with the relevant provisions of the PIPA.

6. Reinforced Measures to Delete and Block Exposed Personal Information

In case of a data breach, the Korea Communications Commission ("KCC") or the Korea Internet & Security Agency ("KISA") may request the IT service providers to delete or block access to the leaked personal information. Failure to take measures accordingly shall be subject to an administrative fine of KRW 30 million or less.

7. Obligation to Notify in case of Collection of Personal Information by Deception/Fraud

Upon becoming aware that personal information was fraudulently collected, the respective IT service provider must notify the victims and take the necessary measures.

8. Notification Requirement for Telemarketers

Unlike other advertisers that send marketing information through electronic means, telemarketers as defined under the Door-to-Door Sales, etc. Act (i.e., telemarketers engaged in the business of over-the-phone sales) were previously exempt from the obligation to obtain opt-in consent to send marketing materials or contact consumers for marketing purposes. While this exception is still intact, the amended law now requires telemarketers to notify the consumer of how the telemarketer acquired the consumer's contact information in order for the telemarketer to be able to avail of such exception. (Note: Telemarketers whose sole purpose is to inform or promote a product or a sales event, without the possibility of concluding a sale agreement over the phone, are not considered telemarketers for the purpose of this provision and are subject to the opt-in consent requirement.)

9. Classification of Types of Overseas Transfer and Enhanced Penalty

The concept of "overseas transfer" was further specified into "third party provision", "processing", "entrustment" and "storage". In each case, consent of the user is required in principle. However, in the case of overseas entrustment or storage that is necessary for the performance of contract relating to the principal service of the IT service provider and necessary for the convenience of the user, the IT service provider may forgo obtaining consent if the following items are disclosed in the privacy policy or otherwise conveyed to the user (by email and other means specified under the presidential decree):

(i) Items of personal information to be transferred overseas;
(ii) Recipient's country, time and method of transfer;
(iii) Name of recipient (in the case of an entity, the name and contact information of the CPO); and
(iv) Purpose and retention period of the transferred information

Further, while there were previously no grounds to penalize for violating this provision, the amended IT Network Act now imposes an administrative fine in the amount of up to 3% of the revenue generated by the IT service provider in connection with the breach.

10. Penalty for Non-performance of Corrective Orders

Under the amended IT Network Act, non-performance of corrective orders issued by the Ministry of Science, ICT and Future Planning or the KCC in connection with a violation of the IT Network Act shall be subject to an administrative fine of up to KRW 30 million.