THE
NATIONAL LAW REVIEW

Amendment to the Personal Information Protection Act Passed in the National Assembly July 6, 2015

Monday, August 3, 2015

On July 6, 2015, the *Korean National Assembly* passed a bill containing several amendments to the ***Personal Information Protection Act (PIPA)***. This bill (the Amendment Bill) combines a number of major provisions from nine previous different bills – *e.g.*, one introduced in 2013 and eight proposed in 2014 following the massive data breach of three major credit card companies that occurred in January 2014 (the Credit Card Company Data Breach). Although the amended version of the PIPA (the Amended Act) will take effect upon its promulgation (yet to be determined), most of the provisions that will significantly affect the obligations and responsibilities of data handlers are scheduled to take effect either a year after the Amended Act's promulgation or on January 1, 2016. For timely compliance with the amended law, companies processing customer or employee data need to keep an eye on the respective effective dates of provisions of the Amended Act that are particularly applicable to them.

Article By
Privacy and Data Protection Practice Group
McDermott Will & EmeryOf Digital Interest
Communications, Media & Internet
All International

1. Significance of the Amendment

The PIPA was adopted in 2011, among others, to protect the privacy of individuals and their personal information from unlawful collection, leakage, appropriation and misuse. However, even after the PIPA's enactment in 2011, large-scale data breaches were not uncommon, and the Credit Card Company Data Breach last year was the final straw that prompted a call for stricter data protection and privacy regulations across the board to raise awareness of the significance of data protection and security and potential serious risks. The Amendment Bill keeps pace with the stricter rules of the recently amended version of the Utilization and Protection of Credit Information Act.

More specifically, the Amendment Bill extends stronger protection measures to individuals affected by data breaches by providing for punitive damages and statutory damages. Further, heavier penalties are imposed on those who violate certain provisions of the PIPA, and illegal proceeds generated from such violations are subject to forfeiture and collection. Whereas the current version of the PIPA provided for the recovery of damages in the event an individual's personal information was stolen, lost, leaked, falsified or damaged, the Amendment Bill explicitly prescribes "fabrication" of personal information as an additional type of data breach, so that affected individuals will also be able to claim damages if their personal information is fabricated. The Amendment Bill also awards broader authority to the Personal Information Protection Committee (PIPC) to address loopholes relating to the practical operation of the PIPC in the PIPA, and provides for the legal grounds for the designation of institutions for data protection certification. Overall, the Amendment Bill contains provisions that increase the level of penalties imposed on violators.

Some of the key changes to the PIPA pursuant to this amendment are summarized below.

2. Adoption of Punitive Damages and Statutory Damages Provisions

The Amendment Bill deletes Article 39(2) of the PIPA which sets forth the mitigating circumstances of a data handler's liability for damages incurred by a data subject whose personal information is mishandled. Furthermore, under the Amendment Bill, if a person suffers damages due to his/her personal information being stolen, lost, leaked, fabricated, falsified, or damaged due to the data handler's willful misconduct or gross negligence, the

court may award the victim punitive damages of up to three times actual damages (Article 39(3)); *i.e.,* the "punitive damages provision"). Statutory damages of up to KRW 3,000,000 (approximately $3,000) are also available to those whose personal information is stolen, lost, leaked, fabricated, falsified, or damaged due to the data handler's willful misconduct or negligence (Article 39-2). By holding the data handler liable for punitive and statutory damages, the Amendment Bill increases the level of responsibility placed on those handling personal information and introduces stronger measures for redress.

3. Heavier Sanctions Imposed on Violators; Illegal Proceeds Now Subject to Forfeiture/Collection

A person who falsely or by other fraudulent means or methods acquires personal information processed by another person and then provides such personal information to a third party for profit-seeking or other illegitimate purpose will be subject to imprisonment of up to 10 years or a fine of up to KRW 100,000,000 (Article 70(2)). Meanwhile, if personal information is stolen, lost, leaked, falsified, fabricated, or damaged because the data handler failed to implement the necessary security measures for the protection of personal information, then he/she will be subject to a fine of up to KRW 20,000,000 (whereas so far under the PIPA, the maximum fine amount is KRW 10,000,000) (Article 73(1)). The Amendment Bill now also allows for any criminal proceeds that a person acquires from the illegal distribution or the like of personal information to be confiscated or collected by the courts (Article 74-2).

4. More Authority Awarded to the PIPC

Under the Amendment Bill, the PIPC is entitled to: (i) recommend improvements of policies and systems, (ii) inspect whether the recommendations are being implemented properly, (iii) request the submission of materials (Articles 8, 11(1) and 63(4)), and (iv) appoint or commission mediators to the Personal Information Dispute Mediation Committee (Article 40(3) and (4)). Meanwhile, the PIPC is allowed to directly handle matters that are necessary for settling disputes (Article 40(8)).

5. Statutory Basis for PIPL

The Amendment Bill provides a statutory basis for using the Personal Information Protection Level (PIPL) certification system (which was under the control and supervision of the National Information Society Agency) as a legitimate means for determining whether the safeguards and measures taken with regard to personal information processing are in compliance with the PIPA (Article 32-2). The Amendment Bill also provides a statutory basis for marking and advertising the substance of the PIPL certification that is duly obtained (Article 32-2(6)). As such, more entities are expected to utilize the PIPL certification system that was introduced in 2014.

Conclusion – Significance of Advance, Ex-Ante Compliance Checkup

Following the amendments to the Act on Promotion of Informemation and Communications Network Utilization and Information Protection, and the Credit Information Act in the wake of the Credit Card Company Data Breach, the Amendment Bill represents one of the final steps by Korean legislators to revamp Korea's privacy-related laws and regulations. The implications of these amendments are far-reaching, as they signify the adoption of legal remedies such as punitive damages and statutory damages, and the implementation of various new regulatory measures across all areas involving the processing of personal information, not just information and communications technology and finance. Apart from the fact that heavier sanctions are imposed on companies for failing to adequately protect the personal information of its employees and customers, many companies will now be forced to revise their everyday practices and policies for handling personal information in order to meet the stricter requirements under the amended laws. As such, companies are now more than ever expected to perform advance inspections of their personal information protection measures in place and make any necessary improvements, in addition to utilizing various certification systems such as the PIPL.

Kwang Bae and Hwan Kyoung Ko are the authors of this article.