Recent Issues of Data Protection Regulation in Korea

The Personal Information Protection Act ("PIPA") was enacted as a general law of personal information in March 2011 to fulfill the need for presiding rules to govern personal information protection. In fact, there have already been a number of special laws governing personal information protection in various special areas and cases, such as The Act on Promotion of Information and Communications Network Utilization Information Protection ("Network Act") governing information and communications services, and the Use and Protection of Credit Information Act ("Credit Information Act") governing personal credit information. Special laws prevail over the general law, when in conflict with individual articles of the general law.

Despite the overhaul of the legal system, large-scale personal data leakage cases involving large corporations and commercial banks have been reported in increasing numbers. Some cases are the result of external attacks, but many of the data leakages were due to the misconduct or negligence of the employees of the companies in question, or mishandling of information by the trustees who were entrusted with business affairs related to personal information. Of particular note, the trustees of personal information have been the most common source of leaks.

Examples

- An oil refiner in Korea entrusted the operation of its customer service centers to its subsidiary. Some employees of the subsidiary misappropriated and attempted a sale of massive amounts of the personal data belonging to its Bonus Card members.

- In a report regarding a leak of customer information from a Korean branch of a foreign bank, an employee of a contractor hired to develop data processing systems allegedly sold approximately 103,000 pieces of customer information to marketing companies. It was reported that the

employee had been facing personal financial problems.

- About 100 million credit card holders' personal data from three credit card companies in Korea was leaked through an employee of a third party vendor. The Financial Supervisory Service verified 85 million cases of the total cases of leaked personal data reported in relation to this incident.

Duty to Take Safety Measures

Article 29 of PIPA states, "A personal data processor ("Processor") shall establish an internal administration plan, keep access records, and take technical, administrative and physical measures necessary for securing safety, as prescribed by Presidential Decree, in order to prevent personal information from loss, theft, leakage, alteration or damage." Article 73 of PIPA imposes criminal sanctions on corporations which do not fulfill those duties subscribed in Article 29, and thereby fail to prevent information leaks. After recent data leakage cases, large Korean companies are building internal compliance protocols such as control of employees' carrying in or carrying out of portable IT devices, limiting access to certain areas, restricting personal email or internet usage at the office, regular and unannounced monitoring of safety measures.

Entrustment of Personal Data Processing

The Processor may provide a third party ("Recipient") with personal data, or the Processor may entrust a third party with the processing of personal data. Even though personal information can be handed over to the third party for either purpose, the key factor that determines the application of the regulations is whether it was a provision of data for the benefit of the Recipient or entrustment of data processing for the benefit of the Processor.

Entrustment of Data

Article 26 of PIPA states that "(i) a Processor, as a truster, shall educate and supervise a trustee to prevent the personal data of a data subject from loss, theft, leakage, alteration or corruption due to the entrustment of affairs, (ii) when liability to pay compensation arises as a trustee violates this Act in the course of managing personal data in connection with the entrusted affairs, the trustee shall be deemed an employee of a truster." In other words, a truster is vicariously liable for any breach committed by a trustee. However, there are two defenses available to the truster, (i) proof that the truster exercised due care in the appointment of a trustee and the supervision of the undertaking, or (ii) a showing that the damage would have resulted even if due care had been exercised.

Article 25 of the Network Act has a provision similar to Article 26 of PIPA, whereas relevant articles in Credit Information Act limit the qualification of trustees, and hold trusters jointly responsible for the conduct of their trustees.

Provision of Data

In the case of provision of personal data, under Article 17 of PIPA, the provider must obtain the consent of data subjects—unlike other business entrustments, which requires only publicity or notification of the outsourcing contract. The related laws, however, do not require a provider to exercise any supervision over, or provide education to, a recipient. In addition, except under special circumstances, providers are only held accountable for their own conduct and are not responsible for their recipient's unlawful behavior.

Transfer of Personal Data Out of the Jurisdiction

With the advancement of technology and globalized business, many activities involving personal or sensitive data are transferred across multiple jurisdictions. Restrictions against the transfer of personal data out of the jurisdiction are commonly found in many data protection laws.

According to PIPA, additional consent of the data subject must be obtained when there is a provision of data out of Korea. Meanwhile, the Network Act requires the consent of the data subject for any transfer of personal data out of Korea, including entrustment of data processing and data aggregation following a business transfer.

Although Korean Financial Supervisory Commission introduced regulation on financial institutions' transfer of personal data out of Korea, there have not been any noteworthy court decisions regarding the issues of transfer of data out of Korea. Yet, with discussions on data localization gaining a driving force, particular attention and continued monitoring of the development of the issues is warranted.

Damages and Punishment

Data leaks due to any violation of related laws can lead to a claim for damages by a data subject, as well as criminal punishment if it constitutes a criminal activity. In most cases, however, the damages have been limited to small amounts of compensation for the emotional distress suffered by victims of the data leaks. Furthermore, a data subject is required to prove his or her emotional distress and suffering caused by the leak of personal data to qualify for compensable damages.

Recently, statutory damages have been introduced in the amended Network Act. An affected data subject may claim reasonable damages of up to KRW 3 million for each case instead of proving actual

damages. The court may acknowledge a reasonable amount of damages within the statutory limits in consideration of the defense(s) claimed by the defendant company and the results of the investigation. Several proposed amendments of PIPA and Credit Information Act calling for introduction of similar provisions is under consideration.

Conclusion

Complying with the laws and regulations governing the protection of personal data of consumers is critical in conducting corporate business. Data leakage cases to date have shown that the culpable parties leaked personal data both negligently and intentionally. It is crucial to educate all those that are entrusted to handle personal data, both employees and third party trustees, about the importance of data protection and strict compliance with relevant laws and regulations, stressing the consequences of disregarding the laws.

If you have any questions or need assistance in relation to the subject of this newsletter, please contact:

- Jongsoo (Jay) Yoon TEL : 02 316 4040 E-Mail: jsyoon@shinkim.com