Recent trends in data breach and the increase in penalties

The Korean Communications Commission ('KCC') has recently implemented a new penalty scheme that applies to companies which voluntarily report a data breach. Hyun-Jeong Kang, Partner at Shin & Kim, analyses this penalty scheme and the broader regime of penalties and sanctions for data breaches in South Korea.

Data breach is on a steep rise in South Korea. In 2013, an employee of a credit ratings firm, which several credit card companies had entrusted with the task of helping improve their systems to protect client data, leaked personal information of major credit card company's customers. An additional breach was reported in relation to a telecommunication company, which failed to prevent a cyber attack from hacking into personal details of its customers. Personal information leakage is a critical issue, since this information would be possibly distributed to unspecified third parties and be misused in crimes such as identity theft, illegal distribution, spamming and phishing, and cause additional damages to the victims.

In that regard, amendments to personal information protection law were introduced to significantly tighten up sanctions against data breaches. Article 64-3(1)6 of the Information Communications Act enables regulatory authorities to impose an administrative fine on a company, even without proving the causal relationship between the company's inadequate security system and a data breach. Moreover, Article 39-2 of the Personal Information Protection Act 2011 ('the Act') and Article 32-2 of the Act on Promotion of Information and Communications Network Utilisation and Information Protection ('the Information Communications Act') implement statutory damages, which would considerably increase damage compensation for the victims.

While the sanctions against data breaches have been strengthened, the KCC announced, on 21 August 2015, the implementation of a new penalty scheme, which allows companies, that have voluntarily reported a data breach to the KCC, to receive a reduction on the total administrative fine prescribed of up to the 30% ('the New Reduction Scheme'). The New Reduction Scheme might seem quite contradictory to the ongoing trend, which has tightened up sanctions against the violations of privacy laws so far.

The Act and administrative fines

Types of penalties for data breach

Under personal information protection legislation, penalties for data breach are categorised into two types: criminal punishment and administrative sanction. The Act imposes strong criminal punishment for material violation, but imposes an administrative fine for negligence. In addition to the criminal punishment and administrative penalty, the provision of the Information Communications Act also inflicts the administrative fine for data breach.

The administrative fine

The administrative fine is a type of a monetary penalty for individuals who violate or do not fulfill legal obligations thereunder, or is an administrative penalty imposed by administrative agencies to a person who made profit from the violation of an administrative law with the intention of depriving a person of (potential) profit. The amount of the penalty is calculated based on the amount of the profit made from such violations. Therefore, it can prevent companies from violating the law by imposing a potential economic burden. Moreover, the administrative fine follows simple procedures, allowing a quicker and more efficient enforcement of law in comparison with the criminal punishment.

The administrative fine system was introduced to personal information protection legislation in 2008 in order to prevent illegal handling of personal information and ensure the rights of users in their use of information. The KCC is the authority that imposes administrative fines mainly in any of the following cases: collection of personal information without the consent of users; collection of civil information without the consent of users; use of personal information for purposes other than those agreed by users; provision of personal information to a third party without the consent of users; entrustment of management of personal information without the consent of users; loss, theft, leakage, falsification or damage of personal information due to inadequate technical and administrative protective measures; and collection of personal information of a child without the consent of his/her legal representative.

The final amount of the administrative fine imposed for the data breach is fixed after the calculation procedure, which computes the basic amount, obligatory adjusted amount, and discretionary adjusted amount. The detailed procedures and standards are provided in the Standards for Imposition of Administrative fine for Violations of the Personal Information

Protection Legislation. The KCC calculates the administrative fine as follows: first, the basic amount is calculated by multiplying the amount of sales related to the violation by the standard imposition rate. The rate is between 0.5% and 0.9% depending on the severity of the violation. The severity of violation is determined by considering various factors, including: whether it involves intention and/or gross negligence; whether it is for profit; the extent of privacy-related damage due to violation; whether the personal information is exposed to the public; and whether the extent of profits gained from violation was comprehensive.

Second, obligatory adjustment is applied to the administrative fine if there is any reason for compulsory aggravation or mitigation. Obligatory adjustment varies depending on the duration and the repetition of violation: if the duration is between one and two years, the basic fine will be aggravated by 25%, and if it is over two years, by 50%. Inversely, compulsory mitigation is applied for the first violation, in which case the basic fine will be reduced to 50%.

Third, discretionary adjustment is applied to the fine if any of the following is applicable. The KCC has discretion to aggravate or reduce the penalty from the obligatory adjusted amount on the basis of various factors, such as a company's level of efforts made for the protection of personal information, whether a company cooperates with the investigation, and whether it has led the violation. For example, if a company actively cooperates with the investigation, the fine may be reduced by up to 30%. If there is any other reason that deserves consideration with regard to calculating the penalty, the fine may be reduced by up to 10%. However, if a company interrupts the investigation by refusing to provide relevant materials and documents or it makes false statements, the fine may be increased by 30%.

The New Reduction Scheme might seem quite contradictory to the ongoing trend, which has tightened up sanctions against the violations of privacy laws so far

Lastly, the final amount of the administrative fine will be determined after assessing the amount with the upper limit stipulated by law (equal to or lower than three percent of the related sales).

The New Reduction Scheme: new efforts for preventing additional damages

Purpose of the New Reduction Scheme

The New Reduction Scheme grants the KCC the discretion to reduce the administrative fine up to 30% with leniency, if a company voluntarily reports the leak. Though the New Reduction Scheme was newly implemented on 21 August 2015, it is worth noting that it has so far been practically considered during the calculation procedure of administrative fines. As explained above, if there is any other reason, the penalty may be reduced by up to 10% in the third step of calculating the fine. In the past, voluntary reporting was deemed an 'other reason.' Therefore, the significance of the New Reduction Scheme is in the expanded scope of the reduction and their stipulation of leniency for voluntary reporting.

The New Reduction Scheme has not been introduced to ease the burden for the violators but rather for minimising the secondary damage resulting from the data breach. Of course, in some sense, strict restrictions could lead potential violators into bringing additional measures to prevent any breach. But in reality, when an accident of personal information leakage happens, the fear of sanctions may lead violators to cover up the existence of such violation, and ultimately hinder companies from being transparent and timely reaction to these breaches. In this regard, the New Reduction Scheme is for reducing negative side effects of strict regulations for data breach by triggering prompt actions in response to data breach accidents and preventing secondary damages that may result from such accidents[1].

Additional measures to prevent secondary damages

Besides the New Reduction Scheme, personal information protection legislation of South Korea includes additional measures to minimise the damage of personal information leakage. For example, the Information Communications Act requires the information processor to report any leakage of personal information to the KCC, in an effort to prepare countermeasures against the leakage of personal information, and seek measures to minimise any damage thereof (Article 27-3 of the Information Communications Act). The purpose of the above provision is:

1. To warn the information owners of any potential identity theft, spamming or phishing resulting from the misuse of their personal information;
2. To enable the information processors in question to promptly receive help in preventing additional leakage; and
3. To recover the damage caused and ultimately minimise additional damage.

The effect of the New Reduction Scheme

The New Reduction Scheme may serve as a strong incentive for companies in voluntary reporting. Since the administrative fine is an

administrative penalty imposed by the agencies to remove any economic profits gained from the violations, it is calculated based on sales, giving significant financial pressure to the company. For instance, a company representative who commits a data breach shall be punished by imprisonment for not more than five years or by a fine not exceeding KRW 50 million (Article 71, subparagraphs 5 and 6 of the Act). However, as for the administrative fine, it may be imposed within 3% of the related sales, which may lead the amount of fine ranging from several hundreds of millions to several billions in Korean won. Therefore, any company that finds a data breach may report the accident immediately to the KCC, and therefore have an opportunity to have the fine reduced. In addition, this may lead the violators into taking prompt measures to prevent further damages with the assistance of specialised agencies and into preparing for any potential claims for damages. These are also beneficial for the companies in general. Finally, the New Reduction Scheme is expected to provide a significant incentive for voluntary reporting and prompt action of companies with data breach issues, and also contribute to decreasing the scope of damages suffered by the victims by preventing any additional damage[2].

Conclusion

As discussed above, the New Reduction Scheme had not been introduced to ease the burden for the violators but rather for minimising the secondary damage resulting from a data breach. In other words, by clearly stipulating that voluntary reporting will reduce the fine, the New Reduction Scheme would minimise the negative side effects of other previous strict regulations, which could cause additional damage to the victims and eventually companies in some sense.

Meanwhile, the New Reduction Scheme will become a model for other jurisdictions. It is similar to the Leniency Scheme under competition law, which has been used in the USA, EU, Japan and many other countries and it will also be helpful in the data protection context. Of course, the Leniency Scheme under competition law has a different intent to the New Reduction Scheme under personal information protection legislation, in the sense that the difficulty to disclose price fixing or secure evidence of a cartel led to the introduction of the Leniency Scheme. However, a voluntary report of a data breach is still worth considering for many countries, not only because a data breach is hard to detect before secondary damage is caused, but also because it is really important to prevent additional breaches.

Hyun-Jeong Kang Partner
Shin & Kim, Seoul
hjkang@shinkim.com