E-Commerce and the Compliance Issue in Respect of Data Protection*

Park, Whon-Il**

< Contents >

Keywords: data protection, data breach, notification duty, class action, compliance, compliance officer, 개인정보보호, 개인정보침해, 통지의무, 집단소송, 컴플라이언스, 준법감시인.

I. Introduction

In the Information Society, an increasing number of data breach incidents take place at on-line shopping malls, companies, government agencies, and so on. In South Korea, where a national identifier of resident registration number is generally used on the Internet, individuals are exposed to unexpected damage arising out of the abuse, misuse

* This article was presented at the International Joint Seminar by Kyung Hee University Law School and University of Wyoming College of Law under the theme “Major Legal Issues on e-Commerce in the United States and Korea” held at Kyung Hee University, Seoul on May 28, 2010. This work was supported by a grant from Kyung Hee University in 2007.

** Associate Professor of Law at Kyung Hee University and Research Fellow of Kyung Hee Institute of Legal Studies.

(투고일자: 2010.07.22, 심사일자: 2010.08.18, 게재확정일자: 2010.09.09.)

or leakage of personal information. Korean citizens have to submit their own resident registration number when applying for not only the administrative services, but also Internet banking and on-line shopping.[1] When data breach occurs, what kind of remedies are the affected data subjects entitled to? Or what are the Internet service providers obliged to do?

In February 2008, an unidentified hacker[2] with an overseas IP address broke into the website of Korea's largest e-marketplace, Auction. The personal data[3] of some 10.8 million users of Auction were apparently leaked out of the country. An emergency meeting was convened at the company immediately. Afterwards their decision-making turned out to be appropriate and reasonable when the Seoul Central District Court ruled in favor of the defendant in January 2010 evaluating the initial response of the management in the affirmative.[4]

Surprisingly, this ruling was contrary to the general expectations. In Korea, data protection in the private sector is basically governed by the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. (the "Data Protection Act"). Accordingly, while doing business on the Internet, any violation of the provisions of the Data Protection Act leads to claim for damages by the affected data subjects and/or punishment in accordance with the Data Protection Act, as the case may be. So the Internet-based businesses, which usually collect and use personal data, are increasingly concerned about the compliance in respect of data protection.

This article explores a couple of typical cases at home and abroad (II) to examine what kind of responsibility the Internet-based businesses should bear - data breach itself or damage inflicted on the data subject owing to such an incident. This article discusses which compliance the Internet-based businesses are obliged to observe in

---

1) Whon-Il Park, "Chapter 7. Republic of Korea," *Global Privacy Protection - The First Generation*, co-edited by J. Rule and G. Greenleaf, Edward Elgar Publishing, 2008, p.207.

2) The Cyber Terror Response Center of the National Police Agency disclosed a user with an overseas IP address had hacked into Auction's website using a computer worm.

3) The damage to Auction users could be immense, as the leaked personal data included names, resident registration numbers, telephone numbers, and, in some cases, bank accounts.

4) Whon-Il Park, "Wind of change in privacy cases in South Korea?", *Privacy Laws & Business International Newsletter("PLBI")* Issue 103, Feb 2010, p.23.

order to stave off such kind of responsibility (III). Finally, suggestions will be made what legislation is necessary for the enhanced data protection in Korea (IV).

Table 1. Collective Suits Arising out of Data Breach

Date	Incident	Latest Developments
Oct. 2005	Lineage gamers' data were stolen	8,500 gamers whose IDs were stolen by other users filed suit against NC Soft, and succeeded in the first instance.
Apr. 2006	Details of Kookmin Bank customers were accidently leaked	When Kookmin Bank sent a promotional e-mail to its customers, other depositors' personal information was accidently attached. More than 1,000 customers claimed damages totalling three billion won against Kookmin Bank successfully in the first instance.
Oct. 2007	SK Broadband (formerly Hanaro Telecom) customers' data were sold	Hanaro Telecom sold details of seven million customers to several telemarketers for profit. 3,000 customers claimed damages against its successor, SK Broadband. The court proceedings are still going on.
Jan. 2008	Details of Auction users were stolen by an unidentified hacker.	An overseas hacker snatched 18 million customers of Auction, 145,000 victims of whom filed suit against the e-marketplace operator only to fail in the first instance.
Nov. 2008	GS Caltex customers' data were leaked	Employees of a data processing subsidiary of GS Caltex, nation-wide gas distributor, intended to sell CD Roms containing customers' data, but failed. 13,000 victims claimed damages against GS Caltex and its subsidiary, which is in process.

II. Data Breach Incidents

1. Data Breach Incidents and Compliance Issues

In Korea, small or big data breach[5] is a part of daily life as a matter of fact. The resident registration numbers of ordinary Korean citizens could be easily collected on the Internet. As the massive scale data leakage takes place more often than not, the above-mentioned Auction case is not the first one. It's because small on-line shopping malls pay little attention to the protection of customers' personal information while big businesses are sometimes lacking in efficient data control system or effective education of employees.

For the past few years, large scale collective suits have been filed with the court against big corporations and banks at the previous page.

There are three types of data breach: personal information was leaked negligently or stolen intentionally by employees (referring to the cases of Kookmin Bank, SK Broadband and GS Caltex); leaked by outsiders[6] (referring to the Auction case); or both incidents are mixed by inefficient technical safeguards and lack of caution dealing with customers' data (referring to the Lineage case).

Most of the above cases became worse since the businesses in question, with one exception of Auction, dealt with the data breach incidents ineffectively or awkwardly. These situations remind us of the recent Toyota vehicle recalls. In terms of compliance, the above data breach incidents seem to result from the failure to observe the simple

---

5) In this article, data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored otherwise processed in connection with the provision of the information and communications services.

6) In the process of the Auction case, the plaintiffs argued that Auction's firewall was too fragile to block expected hacking efforts by outsiders. But the defendant said that Auction took the measure to notify the affected customers of the incident to prevent subsequent damage, because even the state-of-art firewall was insufficient to defend highly skilled hackers.

codes of conduct or regulations for data protection.

In this context, compliance means conforming to a rule, policy or law in respect of the protection of personal data or consumers in general. An Internet service provider (ISP) or company is required to ensure that personnel are aware of and take steps to comply with relevant laws and regulations.[7] Sometimes, compliance is enhanced to the level of social ethics.[8] In Korea, the International Monetary Fund demanded the Korean government to adopt the regulatory compliance in a package of rescue plan to survive the banking and financial crisis in 1997. As a result, the newly amended or enacted banking and financial acts[9] have installed compliance officers in banks, securities companies, insurance companies and even publicly listed corporations.

In this regard, the compliance officer[10] in a corporation is conducting a different organizational function from the existing audit department, and monitoring on a continual basis the compliance with relevant laws, by-laws and regulations. Compliance covers the regulatory matters regarding data protection.

2. The Auction Case

The Auction case, the largest one in terms of the number of victims and plaintiffs in the ensuing lawsuits, shows the necessity of regulatory compliance. Lawyers were

---

7) See the definition of regulatory compliance, at <http://en.wikipedia.org/wiki/Compliance_(regulation)>. In the United States, corporate scandals such as the Enron case in 2001 have highlighted the need for stronger compliance regulations for publicly listed companies. For instance, the Sarbanes-Oxley Act requires significant tighter personal responsibility of corporate management for the accuracy of reported financial statements.

8) For example, Toyota defines compliance as “Comply with ethics, laws and internal rules/policies in engaging in business” — in other words, not act contrary to society’s rules, nor carry out actions that could be criticized by society.
<http://www.toyota.co.jp/en/environmental_rep/03/comp.html>

9) For example, Article 23-3 of the Banking Act, Article 28 of the Act on Combined Capital Market, Article 17 of the Act on Insurance Business.

10) In this sense, a lawyer or attorney is well qualified for a compliance officer, though it is not statutory.

eager to promote massive lawsuits against Auction in their Internet cafes and blogs, encouraging the aggrieved Auction users to join their actions for damages totalling 150 billion won (US$133 million). The plaintiffs organized in several groups eventually exceeded 145,000. In the courtroom, the representatives of plaintiffs argued the ordinary customers of the e-marketplace fell victim to Auction's negligent administration of computer systems and suffered mental distress whether their personal data could be abused or misused as a result of such data breach. If they succeeded in the massive lawsuit, the compensation money, presumably at the same level as 50 thousand won per person in the Lineage case of the first instance, could reach the amount enough to undermine the corporate financial base.[11)]

On January 14, 2010 after two-year-long courtroom arguments, the Seoul Central District Court ruled that Auction was not to blame. The court ruled, "There's no evidence that Auction was lenient about its security measures against hacking." The court added, "It was not legally mandatory for companies to set up firewalls for their websites, considering that there was low credibility over installing firewalls among businesses at that time." Also the court was believed to take into account how the top management swiftly handled the incident to prevent a possible attack in the future.[12)]

The final result of the Auction case should wait for the higher courts as a number of victims have appealed. The appellate court, however, needs to consider the following questions:[13)]

ⅰ. Have ISPs observed the technical and managerial measures required by the relevant laws to safeguard the personal data?
ⅱ. Have ISPs established reliable firewalls and other security measures against possible hacking incidents?
ⅲ. Does it cost too much to install anti-hacking technologies in view of the latest hacking skills?
ⅳ. Have ISPs discharged their duties to prevent possible attack or threat in the future?

---

11) "Auction is not liable to compensation for data breach" Yonhap News Agency, Jan. 14, 2010.
12) See *supra* note 4).
13) *Ibid*. See also the court ruling, 2009 GaHap 88186.

v. How many users are affected by the incident and how large could the actual damage to the victims be?

The Auction case of the first instance has raised the following questions:

i. Is there wind of change in court rulings, so far, in favor of consumers?
ii. Is a kind of leniency program introduced to data protection?
iii. Is the US-type class action recommendable in the area of data protection?

First, Korean courts in the past used to rule in favor of users who sued a company for information leaks by hacking or secretly selling customers' data to others. So it remains to be seen whether the wind of change in this court ruling will prevail in the future.

Second, the response of the top management was swift contrary to expectations. Auction did not try to cover up, but urged the affected users to change their IDs and passwords as soon as possible, and to be cautious in using the existing telephone numbers and bank accounts. The court of the first instance looked at the defendant's response in the affirmative. It seems to make a good precedent just like the controversial leniency program in case of the violation of the Fair Trade Act.[14] As a matter of fact, a voluntary notification of data breach is the only way to prevent further attacks on privacy and properties. With a low probability of arresting hackers, data breach notification could prompt the victims to be aware of probable abuse and misuse of their personal data. Eventually it could make the leaked personal data useless.

In this context, civic groups as well as consumerism activists demanded that data breach notification be established, and, in failure of such notification, ISPs be subject to considerable amount of damages and/or harsh penal punishment.[15] Also, a

14) It was true that a number of businesses covered up data breach incidents, if possible. But Auction's top management adhered to the axiom, "Honesty is the best policy." This situation resembles that of the leniency program under the Act concerning Anti-Monopoly and Fair Trade (the "Fair Trade Act"). Article 22-2 of the Fair Trade Act grants leniency or reduction of administrative fines to the first person that voluntarily reports illegal antitrust activities or submits evidence thereon to the Korea Fair Trade Commission.

15) "State-level countermeasures wanted to prevent hacking" iNews article, ikokid@inews24.com, Jan.14, 2010.

contingent plan to deal with such a data breach would be in great need.

Third, at present in Korea, the US-type class action applies only to securities fraud cases. So the data protection victims had to file the lawsuits individually. The attorneys as well as the court need to confirm the plaintiffs one by one, and it took a huge amount of papers and time. Accordingly, to ensure the full-fledged data protection and compensation of the victims, it will be necessary to introduce a real class action, where several representatives may file suit to compensate a class of victims of the same incident.[16)]

3. HSBC Switzerland Case

In case of the data breach, there are two ways in which the data subject seeks the remedy. First, when such data breach constitutes a criminal activity, the violator is subject to punishment. Second, the data subject may claim damages against the violator and his/her employer. In most cases, the damages are limited to small amount of compensation for the mental distress. If the victims exceed tens of thousand, the total damages grow to an astronomical figure. When the personal data is illegally transferred to a third party inflicting damage to the data subject, the victim has no problem to claim actual and special damages.

HSBC Private Bank (Switzerland) is now confronted with massive data breach cases. Details on 24,000 customers were stolen by an employee of HSBC Swiss Bank in 2007.[17)] In December 2008, Swiss police in Geneva arrested a French citizen who had been employed by HSBC Swiss Bank for seven years, but he escaped to France. In December 2009, French police, acting on a Swiss warrant, recovered the data from him. The files were returned to HSBC Swiss Bank, but the French authorities retained

16) See *supra* note 4). Opponents argue that the real class action would bring an avalanche of lawsuits and put the Internet-based businesses in jeopardy. However, any measures to improve the proceedings and to reduce paperworks should be sought. This article centers on the issue of compliance in respect of data protection, and rules out the discussion on this procedural issue.

17) James Michael, "HSBC Swiss data breach", *PLBI* Issue 104, April 2010, pp.13-14.

copies and began to investigate approximately 3,000 French taxpayers suspected of evading French taxes by using secret Swiss accounts.

The CEO of HSBC Swiss Bank said they deeply regret such a situation and unreservedly apologies to their clients for the threat to their privacy. When France sent copies of the data to Switzerland, it was reported to have given an assurance that the data would not be transmitted to other countries. However, the UK government allegedly acquired the Swiss bank account details of up to 6,600 Britons suspected of tax evasion.[18)]

The HSBC Swiss Bank's data breach is much larger than the theft from a Liechtenstein bank in 2008. Liechtenstein's LGT Group said in February 2008 that the data were stolen from its subsidiary, LGT Treuhand by a former employee, who sold confidential banking customer details to foreign authorities. The German intelligence service, BND, is reported to have paid €4.2 million for a CD containing information about 2,000 people, 600 of whom were Germans. Prosecutors raided the home and offices of Deutsche Post CEO. He later received a suspended two-year sentence and a €1 million fine for tax evasion. The LGT bank has recently been ordered by a court to pay a German client compensation for not warning him of the data theft earlier.[19)]

The High Court in Vaduz, Liechenstein, has ordered the country's largest bank to pay €7.3 million compensation to a German client for not notifying him that his account details had been disclosed to German tax authorities. If he had known of the data breach, the client could have paid tax voluntarily and avoided the criminal penalties imposed on him for tax evasion.[20)]

4. Lessons to be Learned from Toyota Recalls

It is advisable for an Internet-based business to establish an appropriate compliance

---

18) *Ibid*., p.13.

19) In the United States, six people have now been sentenced for tax evasion based on information provided by the Swiss Bank UBS in 2009. *Ibid*., p.14.

20) *Ibid*.

policy. As mentioned before, data protection-related compliance includes conformity with the relevant laws and regulations regarding data protection, observance of the adequate level of socially required data protection and prompt response to the data breach incidents.

In this regard, the Toyota vehicle recalls in 2009-2010 have shown a good example how to implement an appropriate compliance policy. Until recently Toyota top management put the first priority on the reduction of cost. So the production lines could not afford to correct technical and design errors, if deserving additional cost and expenses. Furthermore, they were negligent in controlling the quality of parts procured globally for the purpose of reduction of cost. It is not surprising that Toyota was not exceptional to the typical pattern shown by Japanese companies, i.e., dilatory initial response, reluctant posture minimizing the problem and poor communication with the public about the problem. Most of all, Toyota adhered to conventional lobbyist strategy concealing its problems rather than implementing the contingent plan and fixing the problems, if any.

There must be analogy between Toyota compliance and data protection related compliance. It means that an Internet-based business may repeat the same mistakes as Toyota, if it pays little attention to data protection-related compliance. When a business dealing with personal data prefers expansive operations to adequate protection, it may sacrifice data protection for the efficient management and cost reduction. So it needs to establish a strict level of data protection when it is going to outsource data processing work, in particular, to an overseas data processor or call center. In case any data breach takes place, all the participants regardless of head office, branches, outside processors or consignees are required to take appropriate and necessary steps to handle the incident pursuant to the pre-established contingent plan.[21)]

21) According to FKI report, some defects in the gas pedal were found only in the foreign-made parts, particularly, supplied by CTS in Canada. Therefore, the essential parts vulnerable to fatal accidents are to be procured from the long lasting and security ensured sources affiliated to the manufacturer. When working with a foreign supplier of parts, it should give the first priority to quality control, and the gradual cooperation is recommendable for the quality control. FKI Center for Large and Small Businesses, *The Causes and Implications of Toyota Recalls*, LSC Report No.25, May 2010.

In April 2010, the U.S. Department of Transportation (DOT) charged Toyota with hiding information related to the company's recall of vehicles with sticking accelerator pedals and levied a US$16.4 million fine, which was an all-time record and the maximum amount allowed by law.[22] Likewise an ISP which intends to cover up any data breach could be subject to a similar sanction.

III. Data Protection-related Compliance

1. What is Data Protection-related Compliance?

As mentioned above, precaution is required pursuant to the data protection-related compliance for the prevention of data breach incidents. For the purpose of internal control, the business entities which are obliged to abide by laws should establish an appropriate compliance policy and guidelines, and install the compliance officer in charge of monitoring and preventing illegal activities of officers and employees. In order to gain the credibility of customers and other stakeholders, ISPs dealing with personal data have to consolidate their management and operational system in a positive way.

In principle, the Internet-based businesses are required to take the following matters into account:[23] First, to formulate and make public the private policy which they are obliged to observe; Second, to designate a chief privacy officer and establish data protection organizational units; and Third, to enhance awareness of data protection of employees by means of proper education and training programs.[24]

---

22) Toyota had reportedly sent instructions to the Toyota dealers in Europe how to tackle with the sticking gas pedals several weeks before it notified DOT of such defects in gas pedals. Yonhap News Agency, April 7, 2010.

23) Hisamichi Okamura, *Knowledge of the Japanese Data Protection Act* 2nd Ed., Nikkei Bunko (岡村久道, 個人情報保護法の知識 第2版, 日本經濟新聞出版社), 2010, p.208.

24) The Korea Internet & Security Agency (KISA) is devoted to education in respect of data protection for business personnel dealing with personal data, making and maintaining websites.

2. Disclosure of Privacy Policy

The Data Protection Act[25] demands ISPs dealing with customers' personal data to establish and make public their own privacy policy or privacy statement[26] which introduces and explains what they will be engaged in for data protection. By providing the data protection-related policy and operational guidelines, ISPs may gain the credibility of the customers as well as the data protection authority and the public.[27]

The privacy policy explains how ISPs are committed to protect personal data of their customers, and makes public what they are doing as regards such personal data. In general, the privacy policy is subject to the deliberation of the Board of Directors and made public in the name of the Representative Director of the company.

In accordance with the Data Protection Act, the privacy policy shall include the followings:[28]

1. The purpose of collection and use of the personal data, particulars of personal data collected and the method of collection thereof;
2. The name (referring to the company name in case of a juridical person) of a person who has received the personal data, the purpose of use, and particulars, of the

---

Major subjects of education include KISA's survey of data protection, implementation of protective measures, contents of technical and managerial safeguards applied to ISPs. <http://www.kisa.or.kr/>

25) In Korea, data protection is ensured in the public sector by the Public Entity Data Protection Act, while, in the private sector, by the Act on Promotion of Information and Communications Network Utilization and Data Protection, etc., the Act on the Use and Protection of Credit Information, the Medical Act and so forth.

26) See Article 27-2 of the Data Protection Act. In practice, there is little difference between 'privacy policy' and 'privacy statement'. The former is oriented to the management policy, while the latter is focused on declaring the policy to the public.

27) Take an example of NHN, Ltd., the largest Internet portal service provider in Korea. NHN says "Subject to the Communication Secrecy Act, Electric Communication Business Act, Data Protection Act and other relevant laws and regulations, NHN has established the privacy policy based thereupon and devotes itself to protect the rights and interests of our users." The privacy policy is hyper-linked from the bottom of front page of its website <http://naver.com>.

28) Article 27-2 (2) the Data Protection Act.

personal data in case the personal data is provided to a third party;

3. The period of retention and use of personal data, the procedure and method of destruction of personal data (including the ground of preservation and the particulars of personal data to be preserved in case of preserving such information subject to the proviso except each Subparagraph of Article 29 of the Data Protection Act);
4. The content of business for which handling of personal data is entrusted and the trustee (including the handling policy statement, if applicable);
5. The rights of users and legal representatives, and how to excise the rights;
6. The installation and operation of the device collecting automatically the personal data like the Internet logon files, etc. and how to deny such device; and
7. The name or a person in charge of data protection, or the department to protect the personal data of users and deal with complaints of users related with the personal data, and the contact points like telephone numbers.

From the viewpoint of consumer protection, as shown above, the privacy policy should take the followings into account:

ⅰ. To ensure the suspension of use of personal data in case of collecting such personal data from the data subject;
ⅱ. To handle the entrusted processing of personal data in a transparent manner;
ⅲ. To help clarify the purpose of use of personal data by the data subject; and
ⅳ. To explain in a concrete manner, if possible, from whom and how the personal data are collected.

The content of the privacy policy varies depending upon what line of business the company is conducting. But one thing should be included, i.e. compliance with the relevant laws and regulations. Sometimes there are two kinds of data protection regimes applied to a company - one with respect to customers, and the other with respect to employees. Accordingly, there should be discrimination as regards to applicable privacy policy between two different types of personal data.[29]

29) Let's assume that a big company operates a hospital for the benefit of officers, employees and their families. In this case, the company has to establish two sets of privacy policy - one for

3. Notification required by the Data Protection Act

Chapter 4 of the Data Protection Act provides for which item and how to notify with respect to the personal data. Upon receiving such notification, the affected subject is entitled to do anything permitted by the Data Protection Act.[30]

Table 2. What is to be Notified to the Data Subjects under the Data Protection Act

Article	Subject	Items to be Notified
§22-1	Consent to the collection and use of personal data	1. Purpose of collection and use of personal data 2. Particulars of personal data collected hereunder 3. Period of possession and use of personal data
§23-2 (1)	Submission of alternative resident registration number	Large size ISP is required to notify applicants of alternative resident registration number so as to become its member
§24-2 (1)	Provision of personal data to a third party	1. Recipient of personal data, 2. Purpose of use of personal data of such recipient, 3. Personal data items to be provided, 4. Period of time for the retention and use of personal data of such recipient
§25	Entrusted handling of personal data	1. Person who is entrusted collection, retention, processing, use, provision, administration and destruction of personal data, 2. Description of job which has been entrusted to trustee
§26 (1)	Transfer of personal data followed by transfer of business	1. Transferring of personal data, 2. Name, address, telephone number of business transferee, 3. If no more consented by users, how to withdraw the initial consent

the personnel of the company, another for the patient of the hospital. Okamura, *supra* note 23), p.211.

30) The methods of notification shall be, as the case may be, e-mail, in writing, fax, telephone and other similar means of communications. Articles 10 and 11 of Enforcement Decree of the Data Protection Act. For the notification of general affairs, posting on the website is recommendable.

§26 (2)	Notification by business transferee	Personal data acquired from the business transfer
§27-2	Disclosure of Privacy Policy	Details are described in the above "Disclosure of Privacy Policy."

4. Establishment of Internal Control System

The Data Protection Act requires ISPs to install a chief privacy officer (CPO)[31] and secure a responsive management system. In a big corporation, a director is usually designated as CPO and obliged to report directly to the top management what and how he/she conducts for the data protection and other internal control. It can save the manpower and any dispute within the organization, arising out of similar jobs like data protection and risk management.

As a result, a director in charge of compliance and internal control usually performs the duty of data protection with assistance of the staff which supports him/her. The director is obliged to observe the relevant law and the by-laws,[32] and also bears the duty of due care and diligence.[33] So if a director fails to perform the job of data protection required by the law, he/she shall be liable to the corporation for damages.[34] If the director did wrong knowingly or with gross negligence to an individual, the aggrieved party may claim damages against him/her.[35] It may cause a representative suit against the wrong-doing director.

Take an example of multilevel marketing company in possession of personal data of a huge number of customers. A single data breach incident could drive the company to the bankruptcy. Such a company cannot put an emphasis on data protection and compliance with the relevant laws too much.

---

31) Article 27 of the Data Protection Act.

32) Article 382-3 of the Commercial Code.

33) Article 382 (2) of the Commercial Code and Article 681 of the Civil Code.

34) Article 399 (1) of the Commercial Code.

35) Article 401 of the Commercial Code.

Other kind of companies are not exceptional in implementing an adequate level of data protection and internal control system. Even though it is not yet regulated by the law, the duty to notify any affected data subject of data breach is necessary for an Internet-based business to prevent collateral damage caused by such an incident.

5. Advanced Management System for Data Protection

In terms of data protection, some programs such as ISO third-party assessment, privacy mark, etc. are recommended to the businesses dealing with personal data. Sometimes it is useful and effective in support of the existing data protection regime. A big corporation may adopt the highly efficient management system for data protection.[36)]

With respect to compliance issues, it is advisable to introduce systemic data protection in line with the life cycle of personal data.[37)]

Here is a typical telemarketing company. In the first step, it surveys and identifies what kind of personal data its departments and personnel are dealing with. Making a flow chart of life cycle of personal data is useful. Because a company is like a living thing, a department is made and dismantled from time to time, and people come and go almost everyday. So personal data of the company are ever changing day by day.

The start of life cycle is collecting personal data after notifying customers of its purpose of use of such data. It is necessary to check and monitor how to collect personal data and notify customers of its purpose of use. When a customer's order is received via telephone, it is advisable to post the purpose of use at the website. If the acceptance of orders is carried out by means of mail or fax, the purpose of use of customers' personal data should be described on the catalogue or oder sheet like "Please, read the following statement carefully." If the ordering is carried out on the

36) Highly efficient management system (MS) is operative through the PDCA cycle. Pursuant to the policy, cycles of plan-do-check-action repeat. PDCA cycle is reflected on ISO 8001 and ISO 14001. Okamura, *supra* note 23), p.216.

37) *Ibid*., pp.218-223.

website, the relevant page about the notice of the purpose of use should be linked with the on-line order form. In this regard, the catalogue, order sheet or the captured webpage containing such notice should be maintained in evidence for a possible dispute in the future.

If the processing and maintenance of customers' personal data are committed to a third party outside of the company, the company is responsible for supervising the data processor. It is necessary to review the outsourcing contract, check the requirements of the processor, and monitor its performance subject to the privacy policy. It is also advisable to make standard contractual clauses for the data protection. The same applies to the case where customers' personal data are provided to a third party - banks, insurance companies, etc. Sometimes the provision of customers' personal data to a third party, an opt-out scheme or joint use of such data should be incorporated in the contract. All of these things should be put on record, preferably described in operational manuals rather than contained exclusively in internal regulations of the company.

The final step of the life cycle is the deletion or destruction of personal data. In terms of data security, it is risky and costly to retain unnecessary and useless personal data. The period of maintenance and timing of destruction of data should be specified in the regulations. The method of destruction of data should be safe and secure, particularly in case of outsourcing such job. In this regard, on-spot attendance by the supervisory representative or the certification of destruction is required, as the case may be.

6. Implementation and Improvement

For the efficient implementation of compliance system, it is important for the officers and employees to be aware of its importance by means of education and experience-sharing programs. It is also necessary to monitor how such awareness programs are set in motion and whether any improvement is in need.

The organizational unit in charge of monitoring and auditing should be independent from the CPO and privacy policy staff. It functions in accordance with the pre-published auditing plans and relevant auditing rules. The monitoring result should be reported to

the Board of Directors, and any problem found in the course of auditing should be fixed in a proper manner.

By repeating the above cycle of jobs, data protection could be remarkably enhanced to the satisfactory level.

IV. Data Breach Notification Duty

1. Data Breach Notification required by Law

As explained in the above cases, personal data collected and used by the Internet-based businesses or ISPs are vulnerable to data breach incidents such as abuse and misuse of personal data, ID theft, hacking, etc. So the personnel or the company dealing with personal data should bear the following things in mind: First, is the job in question related with personal data and is there any possibility of data breach? Second, how high level of data protection is required by relevant laws? Third, how much does the data subject suffer from the data breach? Is there any possibility of collateral or subsequent damage?

For an instance, it could be sufficient for a small-sized on-line shopping mall to observe the technical and operational safeguards for data protection required by law. But the situation is quite different for a big company conducting large scale e-commerce transactions. It's because a minor incident may topple the business when a large number of users who are allegedly suffering data breach go to law for damages against it. It is required to do more than the technical and operational safeguards for data protection required by law. It ought to notify the affected users without delay of the data breach incident so that they may prevent subsequent damage caused by the incident.

In Korea, such data breach notification is not mandatory. As shown in the Auction case, the voluntary data breach notification may work on the court in a positive way in the lawsuit for damages. If such data breach notification become compulsory, it might

prevent the damage caused by the incident from spreading out and restrain potential hackers from stealing and using others' personal data for economic benefits. It will not be a new burden to ISPs, but a safe harbor from an unseen disaster in the cyberspace.

2. Latest Developments Overseas

On the world-wide scene, California was the first to impose the data breach notification duty in 2002.[38] Since then, 44 states have followed the basic tenets of California's original law: Companies must immediately disclose a data breach to customers, usually in writing. A national standard for data security breach notification has been discussed occasionally in the U.S. Congress.[39]

In the European Union, Germany took the lead,[40] and the European Parliament and the Council have jointly proposed a directive amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, and Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.[41] In the earliest availability possibly in Spring 2011, the amendment to Directive 2002/58/EC could be materialized in the legislation of all Member States.

Recently Austria followed Germany in amending its data protection law to include a

---

38) The California data security breach notification law, Cal. Civ. Code 1798.82 and 1798.29, effective on July 1, 2003, requires "a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information . . . to disclose in specified ways, any breach of the security of the data . . . to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." In addition the law permits delayed notification "if a law enforcement agency determines that it would impede a criminal investigation."

39) See Wikipedia at <http://en.wikipedia.org/wiki/Security_breach_notification_laws>.

40) For the status of EU Member States, see the *Privacy Laws & Business* report on Data Breach Notification Laws in Europe, at <http://www.privacylaws.com/Documents/data_breach_conference.pdf>

41) <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2009-0360>

specific data breach requirement. The newly amended Austria's Data Protection Act 2000 ("ADPA") introduced an explicit data breach notification duty which came into force on January 1, 2010. Furthermore, a fully computerized notification system will be implemented for the Austrian Data Processing Register by January 1, 2012.[42] A new provision was added as Section 24 (2a) to ADPA.

> If a data controller finds out that data from one of its data applications [. . .] has been used in a systematic, grave and unlawful manner, and the data subjects may suffer damage, he is obliged to inform the data subjects of this without delay and in an appropriate form. This duty does not apply if the notification would require a disproportionate effort in terms of the data subjects facing only minor damages, or the cost of notifying all data subjects in question.

The above new provision shows the criteria of data breach is based on the finding of the data controller, and an exemption where the data subject's damage is minor or the cost of notifying all data subjects is too big. However, the meaning of the new provision does not seem to be clear.[43]

An interesting fact is that the Austrian Data Protection Commission neither needs to be informed about a data breach nor is it involved in any other way in such an incident. This, at first, looks like an advantage for companies, but companies might discover that they will have to make decisions without any guidance as to how to inform data subjects about a breach.[44]

Therefore it is necessary for companies to prepare for an emergency case which would require not only a legal assessment of typical emergency scenarios by the legal department, but also cooperation with the marketing department, information technology

---

42) Rainer Knyrim, "Data breach notification duty added to Austria's Data Protection Act", *PLBI* Issue 103, February 2010, p.1.

43) What a "systematic" or "grave" use of data is, whether a "minor damage" indicates the amount of money or the nature of information, or what an "appropriate form" is unclear. Would it be written communication to the data subject's address, e-mail or a telephone call? "Systematic" might mean that it excludes an accidental incident and there is a time constraint in the abuse of the data. *Ibid*., p.3.

44) *Ibid*.

specialists, management, etc. to establish a contingency plan.[45] In other words, it would be the best policy to take risk management measures on the basis of the compliance standards.

3. Data Breach Notification Duty as Compliance Standards

In view of the latest developments overseas, it is advisable for the data protection authority in Korea to positively consider the amendment to the relevant law and regulations.[46] In the long run, however, it is necessary to be grounded in such a law as giving a warning to the information and communications service providers and allowing sufficient compensation for the affected users like the above-mentioned Auction case. At least, ISPs dealing with a large volume of personal information are required to establish compliance standards as follows:[47]

> When the information and communications service providers find out that users' personal data under their custody have been used in a systematic and unlawful manner and likely cause damage to the data subjects, they are obliged to inform the data subjects of the incident without delay and in an appropriate form; *provided, however*, that this obligation does not apply if the damage seems to be minor, the incident is under investigation, or the notification to the affected subjects would cost to much.

V. Conclusion

Appropriate handling of personal data is pivotal to the individuals and companies

---

45) *Ibid.*

46) The relevant provision of the Data Protection Act is Paragraph 1 of Article 28 (Data Protection Measures). The above-mentioned obligation might be added to the technological and managerial measures required by Article 15 of the Presidential Decree of the Act.

47) A newly proposed data protection bill before the National Assembly for the plenary session of 2010 which combines two lawmakers' draft bills and the government's bill is said to include such data breach notification duty.

engaged in e-commerce for the trustful relationship. The strict compliance with the data protection laws and regulations is not for short-term profit but for everlasting relationship with customers. It takes a considerable amount of investment and manpower to establish an adequate data protection system and prepare for data breach incidents.[48)]

Data protection is another element of compliance for a business entity to perform its social responsibility and facilitate communications with customers and other stakeholders. But any wrongful treatment of personal data could result in legal sanctions against the data controller, and huge damage to customers and business alike including collapse of credit and brand names, and finally exit from the market.[49)]

Against these backdrops, individuals and businesses conducting e-commerce transactions in the cyberspace should bear in mind that, if any data breach occurs, they have to notify data subjects of such an incident, and to take necessary measures preventing further damage. In view of foreign legislative precedents, the existing Data Protection Act shall be amended so that it may provide that data breach notification is not optional but mandatory.

Fundamental solution might be restraint on the temptations of data breach. As a matter of fact, the aggrieved party of the Auction case is not only the customers but also Auction, the e-marketplace itself. Since it is increasingly difficult to chase after hackers, it must be advisable to inform those potential hackers of the lesson that unlawful data collection makes no money but criminal punishment. The obligatory data breach notification, which is reflected on the Data Protection Act as well as the compliance manuals would make an efficient solution to the current data protection issues.[50)]

---

48) Data protection is important not because it is required by the relevant laws, but because it is essential for the maintenance of trustful relationship between businesses and their customers. It would lead to the enhanced competitiveness and improvement of corporate value in the long run.

49) Okamura, *supra* note 23), p.226.

50) The problem is what to do with the hard-to-change personal data such as resident registration numbers, wired or wireless telephone numbers, address, etc., when data subjects are notified of the data breach. In this connection, alternative IDs and minimum collection of data are advisable. Some of those data are indispensable to direct marketing businesses. At least, the

References

Rainer Knyrim, "Data breach notification duty added to Austria's DP Act", *Privacy Laws & Business International Newsletter*, Issue 103, February 2010.

James Michael, "HSBC Swiss data breach", *Privacy Laws & Business International Newsletter*, Issue 104, April 2010.

Hisamichi Okamura, *Knowledge of the Japanese Data Protection Act* 2nd Ed., Nikkei Bunko, 2010. (岡村久道, 個人情報保護法の知識 第2版, 日本經濟新聞出版社, 2010.).

Whon-Il, Park, "Chapter 7. Republic of Korea", *Global Privacy Protection - The First Generation*, co-edited by J. Rule and G. Greenleaf, Edward Elgar Publishing, 2008.

_____, "Wind of change in privacy cases in South Korea?", *Privacy Laws & Business International Newsletter*, Issue 103, February 2010.

FKI Center for Large and Small Businesses, *The Causes and Implications of Toyota Recalls*, LSC Report No.25, May 2010.
<http://www.fkilsc.or.kr/info/content.asp?menu=pub&idx=3835&page=1>.

Internet news articles from Naver <http://www.naver.com>, Google <http://www. google.com>.

Wikipedia <http://en.wikipedia.org/wiki/Security_breach_notification_laws>.

Korea Internet & Security Agency <http://www.kisa.or.kr/>.

European Parliament <http://www.europarl.europa.eu/>.

Privacy Laws & Business
<http://www.privacylaws.com/Documents/data_breach_conference.pdf>
Above websites last visited on July 17, 2010.

processing, financial support and payment for illegally collected data should be subject to criminal investigation and punishment.

전자상거래와 기업의 개인정보 관련 컴플라이언스 대책*

박 훤 일**

인터넷 서비스를 이용할 때 주민등록번호를 입력하는 경우가 많은 우리나라에서는 주민등록번호, 주소, 전화번호 등 개인정보의 불법 유출이나 오·남용에 따른 침해사고가 발생할 가능성이 많다. 2008년 2월 우리나라 최대의 온라인 쇼핑몰인 옥션은 컴퓨터 시스템에 외국의 해커가 침투하여 회원들의 개인정보를 대량으로 탈취해 간 것을 알고 지체없이 이용자들에게 이 사실을 알렸다. 후일 대규모의 집단소송이 벌어졌을 때 서울지방법원은 옥션의 대처방안을 긍정적으로 평가하고 옥션에는 책임이 없다며 원고 패소판결을 내렸다.

옥션 케이스는 우리나라 정보통신망법에 따른 개인정보보호에 관한 법규의 준수(compliance)가 얼마나 중요한지 보여준다. 본고는 인터넷기반의 사업자가 어떠한 경우에 책임을 지게 되는지 구체적인 사례를 살펴보았다. 아울러 개인정보를 보관하는 기업들이 책임을 면하기 위해서는 컴플라이언스의 관점에서 무슨 대책을 세워야 하는지, 입법론에 있어서는 마땅한 개선책이 없는지 검토하였다.

전자상거래가 활발해질수록 우리나라에서는 대기업, 중소기업을 막론하고 크고 작은 개인정보 침해 사고가 끊이질 않고 있다. 이들 사건은 기업의 위기관리 측면에서 문제된 기업들의 개인정보 침해사고에 대한 대처가 만족스럽지 못하여 문제가 확대되기 일쑤이다. 컴플라이언스의 관점에서 볼 때 국내 기업들의 개인정보 침해사고는 간단한 행동강령을 지키지 않은 경우도 많다.

우리 법제에서는 아직 요구되고 있지 않지만, 미국 및 독일, 오스트리아의 입법례를 참고하여 해당 업체가 개인정보 침해 사실을 정보주체에게 통지하는 것을 의무화하는 것을 적극 모색할 필요가 있다. 그리 함으로써 개인정보 침해가

* 이 연구는 2007년 경희대 연구비 지원의 결과임.

** 경희대 법학전문대학원 부교수, 경희법학연구소 연구위원, 법학박사.

확산되는 것을 막고, 해킹과 같은 잠재적인 개인정보 침해의 유혹을 억제할 수 있을 것으로 생각된다. 이것은 정보통신사업자에 대하여 새로운 규제와 부담을 지우는 것이 아니라 사업의 존폐위기를 초래할 수 있는 위험을 미연에 방지하고 이용자들의 신뢰관계를 확보하는 유력한 방법이 될 것이다.

In South Korea, where a national identifier of resident registration number is generally used on the Internet, individuals are exposed to unexpected data breach. In such a case, what kind of remedies are the affected data subjects entitled to? Or what are the Internet service providers obliged to do?

In February 2008, an unidentified hacker broke into the website of Korea's largest e-marketplace, Auction. The personal data of the whole Auction users were apparently leaked out of the country. An emergency meeting was convened and decided to notify the whole users of the incident. Consequently, in January 2010, the Seoul Central District Court ruled in favor of Auction contrary to the expectations.

This article explores a couple of typical cases at home and abroad to examine what kind of responsibility the Internet-based businesses should bear. It discusses which compliance the Internet-based businesses are obliged to observe in order to stave off such kind of responsibility. Finally, suggestions will be made what legislation is necessary for the enhanced data protection in Korea.

In line with the latest developments overseas, it is advisable for the data protection authority in Korea to adopt the data breach notification duty for the purpose of warning to ISPs and sufficient compensation for the affected users. At least, ISPs dealing with a large volume of personal information are required to establish the compliance standard of data breach notification. It's because appropriate handling of personal data is pivotal to the individuals and companies engaged in e-commerce for the trustful relationship.