Personal Data Processing and Business Ethics: Personal Data Processing and Personal Data Protection in Business

Munenori Kitahara

(Received on May 9, 2005)

Abstract

In this paper the author deals with the collection and use of personal data in business. He indicates the problems of abuse of personal data. He explains the reason why the problems very often happen. The main reason is that no corporation hires the data protection commissioner. Data protection is one of business ethics.

1. Introduction

For business activity, personal data are collected at any time and everywhere. Individuals have to give their own personal data to receive various services. They must give their personal data to the bank to receive a financial service. They must give their personal data to the super market to receive a commercial service. They must give their personal data to the local government to receive an administrative service. And so on. Personal data also mean "personality data," which expresses the profile of data subject. That is, the image of personality is built with the personal data. And only the data subject has the right to build his own image of personality.

In business, it would be recognized that personal data are mis-registered, mis-outflowed, abused, mis-given and mis-bought. In business side, it would be forgot that data protection of the consumers or clients is one of business ethics. In respect of environmental ethics, we can recognize the obedience.

There is no end to the unlawful disclosure of the customers' personal data and the customers' lists. Recently, in February 2004, an information service provider disclosed the users' personal data for 4,500,000 persons. In this case, any employee could gain access the personal data bank which stored the personal data. An employee smuggled the lists out of the ISP. The company payed 5 US dollars to a user for an excuse. The damage was estimated at about 43,000,000 US dollars.

"Data Protection," it means that individuals have the informational self-decision right. Or the right can be called the right of data protection. The right is different from the right of privacy. Business entities have to perform the personal data processing holding the right in respect. We, Japanese, can't find the right in any laws and cases. But this right comes from the right of personality and is the most important one in the information society. Business entities can't ignore the right even if they improve their performance in business activity. The entities must respect the right of individuals. This is also one of business ethics.

2. Collection and Use of Personal Data

2.1 *Collection of Personal Data*

Business entities collect personal data in various ways. The entities collect personal data from contract documents, questionnaires, commercial monitors, advertisements for a prize contest, information business, or educational organizations — high schools and universities.

By the popularization of the Internet, in these days, entities collect personal data from advertisements for a prize contest using handy phones, or personal computers connected to the Internet. Most customers put in their personal data allured with luxuries. In these cases, giving the answers is the secondary objective, and receiving the personal data is the first objective for the entities.

Restaurants have questionnaires on the tables. In exchange for a discount coupon or a courtesy card, customers give their personal data — name, address, e-mail address, telephone number, family make-up, birthday, wedding anniversary and so on. Restaurants don't let the customers know where the personal data are stored and managed, how the data are processed and used, where the data are transmitted.

Department stores, super markets, gas stations and do-it-yourself stores issue members' cards. Most stores issue members' cards. By using the cards, customers get points. Using the cards means that the card systems record consumers' activities — what they bought, how many goods they bought, how much they paid. This kind of data, of course, is the very personal data.

Computer programs are used for collecting personal data on the Internet. The Internet browser has the small program, Cookie, in the form manager of which Internet users put their name, address, credit card number, place of employment. The user can manipulate the Cookie in some extent. The user can delete the recorded data and suspend the program. But the

browser with suspended Cookie doesn't work speedy.

The Cookie stores all the URL addresses that Internet users visit at their will. Web sites can collect the URL addresses. A user retrieves a weather report of a city, and buys a book by online shopping. The web site stores the information of the city where the user lives and the information of his favorite authors. The web site can apply the information when the user visits the site at the next time.

"Spyware" is a general term for the software that steals the data of site visiting from the computer connected to the Internet. The spyware has a surveillance function. That is, it surveys which pages users visit and how often they visit the pages. The program tells a frequency of visiting a specified page, a frequency and an amount of Internet shopping, hobbies, goods of users, favorite services, an income level, a consumer inclination. These information are effectively used for marketing.

"Web beacon" is a tag which is buried in web pages and HTML-mails. The tag also stores the data of the Internet users. The beacon collects the data of web surfing, and measures the unique user. It also examines if an HTML-mail is opened or not. Most Internet users don't notice the beacon because it is one pixel four sides large and transparent gif. Therefore, it is apprehended that using those programs cause abuse of personal data.

JIS (Japanese Industrial Standard:JIS Q 15001; Requirements for compliance program on personal information protection) describes the following: The collection of personal data shall be subjected to a clearly defined purpose, and shall be limited to the information required to achieve the purpose (4.4.2.1). The collection of personal data shall be conducted by lawful and fair means (4.4.2.2). Personal data which include the following types of data shall not be collected, used, or disclosed. This shall not apply, however, only in the case where the data subject has given explicit consent to the collection, use or disclosure of the data, or where there are special provision in laws, or where it is necessary for judicial procedures to collect, use or disclose the data (4.4.2.3).

2.2 *The Use of Personal Data in Business*

Business entities promptly need the personal data when they will improve their performance in the markets by raising the degree of the exact valuation of customers' reactions to the various prices, qualities, or indications[1]. Business entity needs the personal data, which

1) O. H. Gandy, Jr., The Panoptic Sort: A Political Economy of Personal Information (Japanese), 46 p.

type of customers bought the goods and which type didn't buy the goods. By applying the technology of database marketing, the entities focus their propaganda activities on the customers who pay great attention to their appeals. The personal data of their latent customers who the entities don't know yet, have the very important aspects in need of increasing customers' information[2].

In business, CRMS (Customer Relationship Management System) is introduced and used for collecting and storing the personal data of the customers. In all the sections that have connections with the customers, they can share the information of the customers, contact history. CRMS can collect personal data at any time of marketing, advertisement of goods or services, offer, an offer of goods or services, and aftercare[3]. It is necessary for business entities to grasp their individual customers' sense of value, their preference for goods or services because they would make a more great profit by raising the degree of customers' satisfaction. In this connection, CRMS is consist of CDS (Customers Databank System), SFAS (Sales Force Automation System), and CTIS (Computer Telephony Integration System).

3. Caces of Personal Data Abuse

3.1 *Personal Data Abuse*

Abuse of personal data means that collected personal data are processed, used, transmitted or disclosed for the purposes outside the scope of collection to which the data subject has given consent. Personal data abuse is caused at any steps of personal data processing[4]. That is, it can be caused at any steps of collecting, inputting, registering, editing, matching, transmitting, joining, sending, using, disclosing, correcting, or deleting personal data. Personal data build the profile of personality by joining personal data of the data subject. The data subject would receive a smaller profit if services were given on the basis of the old or wrong personal data.

In the followings, I will introduce some cases of personal data abuse which were reported on newspapers or the Internet. Why are such personal data abuses caused?

---

2) ibid.

3) H. Kitaoka, Disclosure Cases: Personal Information Protection, Q and A (Japanese), Nikkei BB, 2003, 52 p.

4) M. Kitahara, Informatics of Information Society (Japanese), Nishinihonhokishuppan, 2003, 113 p.

3.2 *Wrong Registration of Personal Data*

In a center for personal credit information, an operator made a wrong input of the name of the owner of the construction company instead of the name of the owner of the machine product company because of a homonym. This case can be often caused in Japanese names. The owner of the construction company was already declared bankruptcy. So the owner of the machine product company was refused a financing aid from a bank, so that the company also was declared bankruptcy. The operator misguidedly registered the name of the owner from the Japanese official gazetto. This kind of mistake must have been prevented if the operator would reconfirm the registration to the owner of the construction company.

3.3 *Unlawful Disclosure of Personal Data*

Formerly, a recruit information company sold the student lists to many business entities, which the company collected for offers of jobs from universities from all Japan. An information service company sold the personal data of the contractors disclosed unlawfully by some life insurance companies. An employee of a consumer finance company logged in the host computer on the terminal at the branch office and got the personal data of 200,000 clients. He sold the lists for 30,000 US dollars. It is a problem for any employee to gain access to the personal data bank of the clients and to download their personal data.

The users' lists were disclosed by an agency of the International Telephone and Telegram company, and by an NTT employee. There are many cases where personal data or customers' lists are sold on the Internet. For example, a video rental shop sold the lists of the customers who were in arrears with the rent. The personal data of 220,000 citizens were also sold on the Internet. The data are used in the Resident Registration Network System. The personal data of 90,000 registrants of staff service company were disclosed by a staff sent by another systems building company.

In November 2003, the personal data of the 180,000 members cards of a convenience store were disclosed. In January 2004, the personal data of 323,820 customers were disclosed in a big customer credit finance company. The data is consist of name, birthday, address, sex, married, the phone number of the office. The company acknowledged that the personal data of 2,000,000 customers might be disclosed.

In February 2004, the personal data of 4,600,000 Internet users were disclosed by an information service provider. A staff downloaded all the data into the DVDs and CD-ROMs. The staff worked at the customer support center and was in the position to read and

retrieve all the contractors' information. At that time there stored the data of 6,700,000 contractors in the personal data bank. The access right was given to 135 staffs with identification who were system building engineers of the provider and system engineers sent from a staff service company.

3.4 *Personal Data Disclosed on the Internet*

These cases are that any Internet user can see the personal data of others.

In January 1998, the personal data lists of 90,000 registrants of a big staff service company were disclosed and sold on the Internet. The lists were consist of name, address, phone number, birthday, and the grade (A,B,C) of the face and figure. A dispatched staff as a system engineer committed the criminal action ("Mainichi DIGITAL Today").

The on-line signature lists of a staff service company were disclosed on the Internet. The web site was built for supporting resulting activity of handicapped people. For 28 months any Internet user could see the personal data. The data are consist of name, address, telephone number, e-mail address, disabled person, sex, age ("Mainichi DIGITAL Today").

3.5 *Wrong Sending Personal Data*

In advertisement of new goods or services, personal data were sent to all the members, so that any member could see the personal data of all the others. This case is caused of wrong operation of the person in charge of the mail system.

In October 2000, for a new product advertisement, Sony Creative Products sent the e-mail to 3,000 customers, which included the e-mail address lists of all the 3,000 members. The e-mail staff carelessly sent the lists as the annex files ("Mainichi DIGITAL Today"). An e-mail address is also one of personal data, and the staff forgot the importance of personal data.

In October 2000, for a new service advertisement, ANA Hotel sent an e-mail to 1,500 customers. The e-mail included the names, and the e-mail addresses of all the customers ("Mainichi DIGITAL Today"). The carelessness of the staff caused these cases.

4. Business and Personal Data Processing

4.1 *Personal Data Disclosure and Business Risks*

Internet business doesn't spread as one expected because Internet users entertain some apprehensions about the use and the management of their personal data which they must give

to in the on-line shopping.

I feel doubt that business entities have a clear consciousness in collecting, using and storing the personal data of the customers. For business entities personal data is an information property. The loss of the information property entails the loss of the business entity. In many cases, the business entity paid 5 or 10 US dollars to the customer for expressing regret. An information service provider paid 40,000,000 US dollars.

If a business entity causes the disclosure of personal data, it exerts a serious influence upon the entity itself. The followings can be supposed[5]. a) The entity has a rush of inquiring from individual, related entities, connections, or media and the entity is overtasked with correspondence and situation explanation. b) From connections, suspending business, warning the improvement, prohibitting the transactions. c) Prohibitting the transactions from the business quarters, and the investigation from the labor unions. d) The obedience to the improvement order by the complement authority. e) Dealing with the require of regret, compensation from aggrieved individuals, and the stockholders' class action. f) The retirement of employee who has a lower sense of belongs or motivation. g) A fall of stock price. h) The aggravation of the business results. i) Bankruptcy.

4.2 *Business Activity and Personal Data Processing*

In information society, personal data processing is indispensable for all the business entities. Some entities proceed personal data for business, others for personnel management. In this sense, no business entity needs personal data processing. If a business entity makes unlawful personal data processing, it causes the bankruptcy of the entity. This is the information age.

Personal information protection law as well as JIS (Japanese Industrial Standard) doesn't prohibit the very personal data processings. Otherwise, personal data processing is recommended by the law and the standard in the way how it constitutes no infringement of individuals' rights or profits. Most business entities have not invested in the personnel and physical installations for the policy of personal data protection, that is, the preventive measures of abuse of personal data. It is a serious question that business entities have had no correct understanding upon the personal data protection.

For the business entities which are indispensable for the personal data processings, the law

5) Japan Network Security Asociation (ed.), The Security Implement Manual for a Countermeasure of Personal Information Protection Law (Japanese), Impress 2003, p. 21.

and JIS standard might restrict the data processings. Is it right? The entities could have made the data processings without limits. From now the entities must make the personal data processings within the limits of the law and JIS standard. That is, the entities must make the data processings under the consideration of the data protection. It is the business ethics, and it brings profits to the business entities.

5. JIS Standard and the Law on the Personal Data Protection

5.1 *JIS Standard Limitation on Personal Data Collection*

JIS Standard means "JIS Q 15001 (1999): Requirements for compliance program on personal information protection." In the section 4.4.2, "Measures concerning the collection of personal data" are prescribed as follows: "The collection of personal data shall be subject to a cleary defined purpose, and shall be limited to the information required to achieve the purpose." (4.4.2.1) In the subsection 4.4.2.4, the standard prescribes "Measures for collecting personal data directly from the data subject." When the business entities collect the personal data directly from the data subject, they must obtain the data subject's consent concerning the collection, use and disclosure of the personal data through written notofication or by an alternative method providing at least the information given below or equivalent information. a) the name or title and the department, telephone number, address, etc. of the manager of personal data inside the business entity or his or her agent, b) purpose of collection and use of personal data, c) in the case where the personal data will be disclosed, the purpose thereof, the recipient of the data, the type and nature of the recipient's organization and whether or not a contract has been concluded concerning the handling of the personal data, d) whether the entrustment of personal data is expected, and its purpose, e) the voluntariness of the provision or non-provision of personal data by the data subject and the consequences of not providing personal data, f) the existence of the right to request access to personal data and the right to request correction or deletion therof if the personal data are found to be erroneous following the acccess, and the specific method by which the right is to be exercised. In the subsection 4.4.2.5, the standard prescribes "Measures for collecting personal data indirectly from a source other than the data subject." The business entity also must obtain the data subject's consent concerning the collection, use and disclosure of the personal data through written notification or by alternative method by providing the data subject with at least the information given in 4.4.2.4 a) throught d) and f) above.

5.2 *JIS Standard Limitation on Use and Disclosure*

In the subsection 4.4.3, JIS standard prescribes, "Measures for the use and disclosure of personal data." The subsection 4.4.3.1 prescribes "The use and disclosure of personal data shall be limited to the purpose to which the data subject has consented."

If this standard applys to the CRMS, it becomes an issue from the point of the data protection principle[6]. When the business entity collects the personal data, the information protection law requires no data subject's consent, but notification or proclamation of the purpose of collection and use. On the contrary, the business entities can operate CRMS by notification or proclamation of the purpose. When the purpose of data collection is the users' registration, customers' registration, repair registration, or questionnaire registration, it is not clear whether the entity can use the data directly for the other purposes.

6. Installations for Data Protection

6.1 *The Concept of Data Protection*

Data protection, in the broad sense, is composed of two concepts, data protection (in the narrow sense) and data security, from the point of view of the object to be protected and the way to protect it. Data protection is aimed principally at protecting "individuals," and the data security is aimed principally at securing "data." In other words, data protection is aimed at protecting the personality data of individuals in the personal data processing.

Data protection is derived from the object of protecting individuals and their private sphere in the data processings. Therefore, the laws and JIS standard of data protection regulate the legal relationships among the data subject, the data manager and the data user. In the legal relationships between the data subject and the data manager, the norms regulate the rights of the data subject and the duties of the data manager which are derived from the principle of data protection. The norms also regulate the right-duty relationships between the data subject and the data user. Between the data manager and the data user, the manager has the authority to supervise the performing of the duties of the user for guarantee of the data subject's rights. Under the concept it is important what (who) to be protected. Data ptotection can be realized by the legal norms as JIS standard.

6) Kitaoka, ibid.

6.2 *Data Security*

Data security means security of data, therefore, security of data media which store data. Under this concept, it is a problem how the data are to be secured. Data security can be realized principally by the preventive measures of data theft, data destruction, data counterfeit, or data abuse. Therefore, data security can be realized by the technical measures which prevent the data destruction, the data alteration, the data abuse, as well as the organizational measures which prevent unlawful personal data processings. As data security, the main activity is to keep the security of all the data files and the computer support system including the computer programms. The preventive measures of data theft and data destruction are the security measure which defends the data storage against natural disaster, and the strict access control to the data strage room. The data security measure embraces the measeures which defend the data media against deterioration, and the measures which defend the data files against destruction through unlawfull access by software. The measures which defend personal data against an unauthorized use or miss-manipulation of computer terminals are the limits of competence to deal with paersonal data, and the measures limit usable personal data by encryption or using identification method.

Data security can be realized directly by technological and organizational measures, and legal norms support it indirectly. As mentioned above, the data protection is aimed at protecting individuals by defending personal data against the abuse in personal data processings, and otherwise, the data security is the technical and organizational measure which defends personal data against the abuse in personal data processings. However, data security can become a data protection measure when the data abuse causes infringe of private sphere. That is, data security is the method of realizing data protection, and data protection is premised on data security.

6.3 *Data Manager*

A data manager is a person who is responsible for all the personal data processings of the entities. The data manager also is a norm addressee of data protection law and JIS standard. The manager burdens the most serious duty of care because he must process fairly and reasonably the personal data, and observe the personal data protection law and JIS standard.

First, it owes the obligation which corresponds to the right of data subject mainly vis-a-vis data subject. It is the obligation which offers information concerning the data regarding the

individual for using the access right of data subject. Namely, you must inform on the type and contents etc. of storage private data to a data subject. In addition, when error of the data is discovered, correction, elimination or blockade of the data measure must be devised on the basis of the correction right of the particular individual. In addition, the case of installation of the private computer system is reported you can assign the obligation which to the supervisory authority or the supervision concerning the important matter execution of permission or the notification.

The last obligation is the duty of the data administrator. When error of the data is discovered, the data manager, with authority, must correct that error, or eliminate all the data that includes error, or must blockade the data files. In addition, when inaccuracy, or the invalid data was offered to the third party, there is an obligation which notifies the effect to the third party. Furthermore, the data manager must devise the technological organizational measures for data protection, and the data security measures.

6.4 *Data Security Measures*

Data security means to secure data, data files, computer programms, and computer systems. Under the concept of data security, come the technical measures which defend personal data against destruction, alteration and theft, and the organizational measures which defend personal data against unfair data processings.

In applying the data security measures, the proportional principle should be adopted. It is important that the measures must be balanced between the cost and the object to be secured.

(1) Access Control: to prevent unauthorized persons from gaining access to data processing sysytems with which personal data are processed.

(2) Strage Media Control: to prevent strage media from being read, copied, modified or removed without authorization.

(3) Memory Control: to prevent unauthorized input into the memory and the unauthorized examination, modification or erasure of stored personal data.

(4) User Control: to prevent data processing sysytems from being used by unauthorized persons with the aid of data transmission facilities.

(5) Access Control: to ensure that persons entitled to use a data processing system have access only to the data to which they have a right of access.

(6) Communication Control: to ensure that it is possible to check and establish to which bodies personal data can be communicated by means of data transmission facilities.

(7) Input Control: to ensure that it is possible to check and establish which personal data have been input into data processing sysytems by whom and at what time.

(8) Job Control: to ensure that, in the case of commisioned processing of personal data, the data are processed strictly in accordance with the instructions of the principal.

(9) Transfer Control: to prevent data from being read, copied, modified or erased without authorization during the transmission of personal data or the transport of storage media.

(10) Organizational Control: to arrange the internal organization of authorities or enterprises in such a way that it meets the specific requirements of data protection.

7. The Problems of the Personnel Installations for Data Protection

7.1 *JIS Standard and Data Protection Law*

Personal data protection means preventing the abuse accidents of personal data which are expressed before. That is the purpose of data protection. If we consider that the abuse accidents of the personal data occur at the time of personal data processings, it probably does mean that greatly problem exists in the patsy manager and those supervisory supervision systems of personal data processings. The JIS standard describes (4.4.1), "The top authority of the business entity shall appoint a manager within the business entity who shall understand and observe the provisions of these standards and shall give the manager the authority and responsibility to implement and operate the compliance program, independent of any other reponsibility." But, as for stipulation concerning the personal data processing manager, it is not put in the latest Japanese personal data protection law.

At a certain local government, a hierarchical personnel installation for personal data protection is provided, which responds to the supervision business, the data protection controller, the data protection manager and the general data protection manager. They are not working full time. The section chief of each section is appointed the data protection controller, the bureau chief of each bureau is appointed the data protection manager and director of administration is appointed the general data protection manager. As for the data protection controller, first, it can require the proper management of the data and program and record medium, utilization restrictive measures of the transmission data with the communications network and the like and elimination measure and the like of the unnecessary data are assigned obligation. In addition, when they do new data processing concerning

personal data, in advance, the data protection manager must give the notification to the general data protection manager.

7.2 *Internal Control and External Control for Data Protection*

As form of the supervisory authority for data protection, from the ombudsman system to the administrative organization you can think various forms. In these days, we can see many of the supervisory authority which possesses the character of the administrative organ. In Sweden, that is called "The Inspection Board (Datainspektionen)." The data inspection board is one of the central administrative organizations, and is independent in the same as the other central organizations. The Board has the ombudsman role of the general citizen other than execution supervision business of data protection law. In France, "The national commitee for information processing and freedom (CNIL)" is the administrative organ which is independent, and it is not necessary to follow in supervision authority in every hierarchical organizational authority. In Germany, on a proposal from the federal Goverment the Bundestag shall elect "the Federal Commissioner for Data Protection (BfD)." The Federal Commissioner shall, as directed by the Act, have public-law official status with respect to the Federation. The Commissioner shall be independent in the performance of his duties and subject to the law only. In this way, it is required to the supervisory authority for data protection to have the independence, the fairness the in-between position that it does not receive command and supervision from everywhere.

As a supervisory method of the supervisory authority, other person supervision and self-imposed supervision, in other words, you can think the form, external control and internal control. Whether we adopt standardized supervisory system of public and private data processing with the special system outside, or whether you take gradual supervisory system inside on the basis of the principle of self responsibility, we should decide in the range of the data which becomes the regulation object and connection with the other degrees of laws.

Then, from for watching the data protection which has effectiveness, "independent supervision or other person supervision?" that it is not method of the 1 out of 2 alternative which is said, connection of the two forms, namely, the method, "other person supervision and independent supervision" is necessary.

The first business of the supervisory authority, usually, designates that the authority audits "observance of the provisions of data protection law." The duty and the range where authority reaches, as a general rule, should limit to the personal data of automatic data

processing. When the range of duty of supervision expands to the manual data processing, the duty cannot be accomplished appropriately, because the data files of the kind (generally known document information) rises to the enormous quantity, and at the same time, are scattered in wide area. Therefore, as for the range of supervision of the supervisory authority, we should assume that it is limited to the data which is registered by permission or the notification in the case of installation of the personal data processing system[7].

7.3 *Data Protection Commissioner System*

7.3.1 Leakages of Personal Data

From the causes of outflow of the personal data in the personal data abuse incidents which have become clear so far, the primary factors of outflow of the personal data can be described as follows:

(1) Unlawful bringing personal data: Personal data are brought outside by the data processors of the respective company or the other information processing company. They can access the personal data at all the steps of data processings. They can record the data in floppy disks, CD-ROMs, memory cards, handy phones, portable computers and print the data on the paper. Or they can send the data to the other places by a network. In many cases where an organization outsources the procssing of personal data, it may give the information processing campany substantial discretion as to the detailed manner in which the company actually processes the personal data.

(2) The error transmission of personal data by e-mail: At the time of mail transmission, it is accustomed to sending the personal data of others other than this person by the failure of the person in charge. It happens well to the mailing list and when multiple address transmission is used.

(3) Defectiveness of system: Defective of the system of the web site of the company or depending upon design mistake, in Internet user the private data of company possession becomes a state where it is perusal possible.

(4) Defectiveness of access control: From defectiveness of access control, the person who does not have access authority accesses the personal data files, and brings up the personal data outside.

(5) Illegal access: Via network, a hacker invades the system just, and downloads the

7) Munenori Kitahara,The Problems in Japanese Personal Data Protection Law, The Law and Computer No. 8, 1990, p. 74.

personal data files.

(6) Computer virus: A hacker sets up the computer virus which collects the personal data.

(7) Social engineering: It is the behavior which a person illegally gets the ID of others, the password, or the system manager information, with which accesses to the system and the web site.

(8) Defectiveness of management of use: Disclosure of the personal data happens from the risk of the data management in moving the personal data, that is transporting, transmitting, sending the personal data.

(9) Restoring the personal data from the rubbish and the waste: The questionnaire paper of the input being completed without being incinerated there are times when it is picked up.

(10) Theft of personal data: The personal data is stolen from network. Invading the clerk's office, a person steals the personal data on the hard copys. The computer where the private data is recorded is stolen.

(11) Outflow of personal data from consignee: When entrusting the processing of the personal data, the consignee human material equipment of data protection for the insufficiency, occurrence frequency of outflow incident of the personal data is high.

7.3.2 Data Protection Commissioner

In order to prevent many kinds of abuse of personal data, it is necessary to make clear the obligation and the responsibility of data manager as well as to consolidate the control power on personal data processings. Moreover, it is more important for Jpanese business entities to install the personnel who audits the personal data processings. The personnel is named "Data Protection Commissioner." Japanese data protection law as well as JIS standard doesn't describes the personnel.

Business entities must install a data protection commissioner as the audit controlling the personal data processings, when they perform the personal data processings. The data protection commissioner undertakes the supervision of personal data processing of business entities. The commissioner must be given the position which becomes independent from the entities. When the abuse incident of the personal data procesing is serious, the commissioner has the authority which can blockade the personal data processing.

Data protection agency is installed in the nation, the data protection commissioner of the nation is arranged there. Data protection bureau is installed in the local goverments, the data protection commissioner of the local governments is arranged there. The data protection

department is installed at business entities, the data protection commissioner of the entities is arranged there.

7.3.3 Qualification of Data Protection Commissioner

It is necessary to provide the qualification system of the data protection commissioner. The data protection commissioner, for the duty accomplishment, must be a person of noble character who holds legal knowledge and technical knowledge sufficiently[8]. In order to prevent the outflow and leakage of the personal data to outside, the fact that the primary factor of those outflows and leakages is removed is the most effective plan of data protection and data security. Therfore, the legal, technical, and management knowledge is required to the data protection commissioner who audits the personal data processings and the abuse of personal data.

First, knowledge of data protection law is required to the commissioner as a legal knowledge. The commissioner also must have the knowledge of the data protection ordinance in the local governments. When overseas circulation of the personal data is done frequently, also the knowledge is required to the commissioner concerning the data protection law of related foreign countries. In addition, the commissioner has to have mastered the JIS standard, the guideline and the guide for personal data protection.

Next, the commissioner must have the technical knowledge which relates to data security and the knowledge which relates to the concrete measures of data security. Namely, the special technical knowledge is required to the commissioner, which relates to the personal data processing system, computer network and network security. The commissioner has masterd the tecnical knowledge of data entry unit, data output device, computer peripheral unit, data transfer unit, data transfer media, external data storage unit, computer network, network topology, threat to network, and network security.

7.3.4 Authority of Data Protection Commissioner

The data protection commissioner belongs to the business entity, but, the position is independent. The commissioner has owed quite heavy responsibility. Therefore, the authority is very firm. As the strongest authority, it is possible even to temporary blockade or abolition of personal data processing of the post entity. As a general authority of the data protection commissioner, we can think those below.

(1) Application authority of technical knowledge and technology for personal data

8) Reinhard VoSSbein, Die Organisation der Arbeit des betrieblichen Datenschutzbeauftragten, DATAKONTEXT 1997, SS. 47ff.

protection.

(2) Audit authority and entering investigation authority for data protection and data security.

(3) Advice authority to the entity exectives concerning the problems of data protection and data security.

(4) Prosecution authority to supervisory office concerning the doubt problems.

8. Conclusion

If business entity aims toward the enlargement and the development in information society, it is important for the entities to realize the personal data protection of the customer and the consumer. If personal data processing is indispensable in the business, the measures for personal data protection must be designated as perfect ones. That is one of business ethics. The entities must protect the personality right of the individuals.

The business entity possesses personal data and personal information of enormous quantity. The personal data and the personal information are portion of information property for the entities. In the same time, those data and information should be the trade secret. As for the data and information, when they are once disclosed, they stop being a trade secret. In order for the data and information to be called a trade secret, they require strict control enough to be prerequisite in secret treatment.

As for the unlawful disclosure of personal data, it is impossible for the data subject to reset to the origin. In the case of the personal information disclosure, we can't hope the perfect recovery. This is the very character of information. At the beginning of eighties, the first personal information protection bill had been discussed at the National Diet. The bill became failure to act and a waste plan. "The problems have not been realized yet. We think that we, Japanese, have no necessity of such a law." The Assemblymen shouted unanimously. As for personal data protection, the meaning of data protection had been lost if the problem has been realized. Personal data protection is meaningful in beforehand prevention of abuse of the personal data.

At the time of data protection, after all, lastly, the problem of personnel installation for data protection is left. When, perfection execution of law and JIS standard even, the personnel installation is necessary, which audits the performance. The data protection manager who bears the whistle-blowing role of personal data processing, and the data

protection commissioner who bears the external prosecute role of personal data processing, those prsonnel installation being arranged, complete data protection is actualized for the first time.