Personal data security - a personal perspective:
How the lack of legal framework can affect work

by Nina UGRINOVSKA

This study is developed on the basis of the presentation that took place on 7th April 2004 as a special event of the EU funded Drafting of Trade Laws project. The presentation was entitled "The new framework on security of personal data".

We live in times of very advanced technology, when every information and the access to it, is of utmost importance. Security must therefore be controlled to the maximum in order to prevent misuse for various illegal purposes. This must be done within a clearly defined legal context In this presentation, I shall explain my views on this subject based 15 years of experience working with data and the information sector, participating to many seminars and having kept abreast with expert literature.

In the 21st century, the most expensive product is the information that is available on the market. By having the right information at the right time, it is possible to maximize your goals. Therefore, information as such is subject to various forms of misuse to acquire personal benefit, to make profit, to have a competitive edge but equally to cause intentional damage. Information can also be used just for pleasure and fun. In this context, the important issue is the security of the information as well as the ability to sanction and be protected from unauthorized and illegal use of the information. If somebody breaks into our apartment, if our car is stolen, if we are mugged on the on the street, we can always report these cases to the police. Yet if information is stolen and is afterwards misused, we have nowhere to ask for help or for legal rights. Furthermore we have nowhere to turn to seek compensation when the damage can sometimes much more serious than the theft of a car. It is therefore of crucial importance that the data and information are protected with a solid legal framework and that safety measures are implemented to prevent any possible misuse. Particular attention must be payed to equally protect electronic and paper data because the results can be equally damaging. I will there address the issues and procedures with regards to the protection and processing of electronic data and information. Information in a database can be the subject of three kinds of attacks: internal ones (employees of an organization), external ones (anyone outside the institution living anywhere on our planet!) and during the transfer through telecommunication systems (from one branch to the other, within one organization, or between various organisations during the process of data and information exchange).

The most frequent and most dangerous attacks are the internal ones. Indeed according to surveys, 90% of all unauthorized use of data are performed by employees of the company he/she is working for or with their assistance. One of the most important precautionary measures in such cases is to setup working procedures and access as well as different security levels. Protection must be on the physical and logical levels. Physical damage of information can occur due to improper handling of the technical equipment, damage or malfunction of the computers, or and accidents (fires, etc…). In such cases, the best protection is to do regular backups of systems and databases. It is also necessary to remotely manage servers on various locations when dealing with more sensitive systems. It is very important to control the quality of the backup (a backup is a reserve copy of all information contained in a single computer) done by an expert. Indeed there are cases when the backups are not only untrue to the original but they are something completely different and therefore useless. By physical protection it is meant that the computer location must be secured from access. All security systems in the network would be rendered useless if

somebody manages to enter the room and physically steal the computer together with all its content! I would also like to mention one more example of badly organized backup. If the media are kept in visible and accessible locations (very often near the computers) that are backed up and a fire breaks out, these are destroyed together with the computer. Therefore, it is essential that these should be kept in specifically designated and secured locations. In other words, strict procedure is necessary and it must be in written form for the entire action of physical security of the information. Every employee must be held responsible if he/she does not comply with the strictly defined rules.

By logical security of the information, we mean its validity. What can go wrong? Because of improper or insufficient knowledge of the application(s) i.e. software, there is always the possibility that some information is entered incorrectly. When the incorrect dat is for example gender, a male employee would receive flowers on women's day! However, much worse can happen and human life can be threatened if a person receives for e.g. the wrong blood type during a transfusion because of a typing error. To avoid these mistakes it is crucial to train properly the employees and to familiarize them with the application they are working on. It is also necessary to restrict strictly the access levels, i.e. who is allowed to enter data, who verifies and confirms the data, who has the authority to modify, erase or read the data. Finally it is important to clarify who is allowed to process these information for further needs. This entire structure must be spelled out in procedures and authorizations, supported by legal norms and regulations. Another important step is to classify data according to its importance. This implies introducing the so-called "four or six eyes" system, i.e. information must be checked and verified at least 2 to 3 times before being entered in the database. If the eye color of a person is entered incorrectly, a life threatening situation will not ensue. However if the unique ID number is entered incorrectly, his/her existence can be transformed into someone else's! .

It is critical to secure the data from external entities or influences (i.e. unauthorized access byhackers or intruders. Their motives can be personal benefit but in the case of hacking it is just about showing that it is possible to access highly secured systems. Hackers or intruders can caused enormous damage if information is destroyed. Illegal intrusions push security system operators to constantly update their security. There are cases of financial thefts or intentional malicious attacks from competitors to demonstrate their superiority, or changes in the data content to avoid sanctions, or to receive acknowledgments or awards. Whatever the reasons for intrusion, it always causes great damage because time can ellapse before the attack is noticed. Often unfortunately it remains unnoticed. These actions can be compared with breaking into somebody's home or companyand browsing and changing the personal information or data. It is an invasion of privacy and a criminal act which unfortunately in the IT environment remains too often unsanctioned. To make matters worse, there is no institution to report these cases and nobody to prosecute these illegal actions. Therefore, no resources should be spared in the field of data security to have maximum monitoring because a single hack or intrusion can have irreversible consequences.

Data transfer through telecommunication infrastructure is a necessity and is constantly taking place. While traveling from one machine to the other, the information is out of our control and easily subject to manipulation. In order to avoid unpleasant surprises during the data transfer, it is necessary to have crypting, coding and security models and mechanisms. While information travels, the data can be easily intercepted and come into the hands of unauthorized persons who can further misuse it. The best option is to sign strict agreements on who is responsible for sending and receiving or to transfer of the information.

All the above problems, issues, procedures and protections need to be carried out and implemented under strict supervision by the company's IT sector employees and need to follow a strict control and to adhere to the rules of the management of the organization concerned. Each head of department must provide a written study for his department on all activities and rights of the employees for the handling of and work with the data in the scope of their assignment. The more obligations are defined, divided and specified, the better the control and security system is. Finally, on top of the pyramid, we have the system administrators and IT personnel who have all the passwords and have access to the entire system. It is necessary to produce a detailed structure of their access in order to make external audit possible. The best option is to divide the passwords in two parts (or to setup more passwords if necessary) and for every change in the system administration to impose the presence of at least two employees. The most dangerous option is when a single system administrator has all the passwords and controls all the access. In this event he is able to make any manipulations with the data because no control is exerted on him.

In order to avoid misuse and to achieve maximum control, each end user must sign that he agrees to and will comply with the security procedures and policies of the organization. He must state that he is fully briefed, informed and familiar with his responsibilities and that he will be held responsible for irregularities. The organization should be able to determine responsibilities (between the supervisor and the employee when procedures have not been complied with. . Or whether the organization should be held responsible because of the incorrect data processing.

The best way to check the handling of the data is to establish daily monitoring of the log files (system logs that have information on its entire activity) and this on 24-hour-basis. These logs need to be updated (revised) by people coming from outside the IT department. It is necessary to define the access time to the system and information. Each activity outside the prescribed time is allowed only with the authorisation and steering of the person in charge. Systems are mostly attacked outside working hours because of decreased monitoring and the absence of system administrators. In the case of an employee's absence (holiday, sick leave, etc.) it is advisable to temporally block his system as a safety measure.

Another important recommendation but unfortunately often neglected is the security of applications and software. All non-licensed and non-standardized software can have backdoor holes which can be intentionally left open by the programmers so they can enter the system and use the data unnoticed. It is necessary to buy the software from ISO certified companies that provide all guarantees for the security, accuracy and processing of the data. These must be implemented in bilateral agreements clearly stating rights and responsibilities. The employees must be forbidden to install any other software on any computer in the network without consulting and approval by authorized persons in the IT department.

In conclusion, a company must ensure better training for the end users, regular training for the IT employees on all new technological achievements, usage of all available resources for procurement of good and secure software. Improvisation should definitely not be applied with IT technology and no costs should be spared because risks and stakes are are too high.