

Best Practice for Data Protection Implementation **

Wherever you live and whether your state/country provides data protection acts or not: if you are in charge of data protection, the following approach is promising and economical:

1. Identify all application programs which are used to process personal data (*1) in your institution (so called "procedures").
 - a) List these procedures (in a "procedure register").
 - b) Describe the personal data or the data types (data concerning the same subject) for every procedure processed in these applications.
Find out who is in charge of these applications (*2), and who has access to the data, as well as what is done with the data and why this is done or has to be done.
 - c) Analyse the registered procedures in order to find out if the requirements (Acts, Guidelines, Policies and Directives) are fulfilled. If necessary, arrange modifications of the procedure or its use with the person in charge.
 - d) Procedures which in case of improper use can cause important damage for the affected person (*3) have to be documented in detail (in a "data file register").
Instead of only describing the "data types", you have to describe the structure of the data base accurately, including the data field level.
 - e) Document the modifications and the claimed/implemented safeguards for (d).
 - f) For particularly sensitive procedures, document also which hardware is used for the data processing. Hardware, configuration, links to the outside (*4) and the people in charge are to be described.
2. Participate regularly in further trainings linked to "data protection" and "privacy". Document your participations.
3. Don't assume that your staff members will acquire "data protection know-how" all by themselves. Train your staff in the principles of the "data protection acts" and their requirements. Pay attention not to go too far into detail. Successive trainings (beginners, advanced, masters, ...) have proved to be reasonable.
4. Let your staff sign a formal obligation concerning the keeping of the respective acts, guidelines, policies and directives. Describe in this formal obligation explicitly the disciplinary punishments.
5. Repeat the points 1 - 4 regularly – at least once a year.
Follow the approach: Plan > Do > Check > Act.

*1: personal data is data from/concerning people: staff, suppliers, customers, patients, clients, retirees, applicants, ...

*2: normally the supervisor of the department.

*3: the affected person is the person whose data is being processed.

*4: Internet, modem, phone connection, CD/DVD-Writer, floppy disk, other removable data medium.

** without guarantee.