Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The Federal Data Protection and Information Commissioner (FDPIC)

A Guide for technical and organizational measures

August 2015

Feldeggweg 1, 3003 Berne
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Table of contents

INTRODUCTION

This guide is an introduction to the data protection risks that can arise in connection with modern IT systems. It is intended help the reader to implement measures to ensure optimum and appropriate protection for personal data. The main data protection topics will also be presented together with the technical and organizational measures associated with them: encryption, anonymization and authentication.

The guide is primarily intended for IT systems managers and those who are directly involved in the management of personal data, whether they are technicians or not. Other interested parties may, however, also find answers to their questions here.

The guide is structured around four main topics – data access, data lifecycle, data transmission and right to information. The aspects that need to be considered in both design and implementation will be presented for each topic. The measures suggested should be taken as general guidelines and adjusted to the circumstances of the specific project and organization involved.

Definitions

Some terminology definitions for a better understanding of this guide are listed below.

Data/Information security

- ***Data/information security*** includes all the measures taken to protect the confidentiality, integrity, and availability of the data/information.

Data protection

- ***Data protection*** includes all the measures taken to prevent unwanted processing of personal data and the resulting consequences.

Information protection

- ***Information protection*** defines the confidentiality levels of information (INTERNAL, CONFIDENTIAL, SECRET) to protect the interests of a country or an organization.

Personal data

- All data relating to an identified or identifiable person is referred to as ***personal data*** *(aka Personally Identifiable Information)***.** They are designated as **non-sensitive personal data**, when these do not hold any particular sensitivity (cf. definition below).

- ***Sensitive personal data*** are data about a person's religious, ideological, political or trade-union views or activities, the health *(aka Protected Health Information)*, private sphere or racial origin, social security measures and administrative or criminal proceedings or sanctions. If the disclosure of such information could result in a high-risk threat, in particular to life and limb of the data subject, it is then referred to as ***hypersensitive*** (vital) **personal *data***.

- A ***personality profile*** is a collection of data to help assess the significant aspects of an individual's personality.

- The ***data subject*** is the natural person or legal entity to which the data refers.

- There are four **risk levels** for personal data:

    1. ***Low risk*****:** Personal data the abuse of which does not have particular consequences. Examples include the first and last name, address and date of birth or any information that has appeared in the media unless it is in a sensitive context.
    2. ***Medium risk*****:** Personal data the abuse of which could have a severe impact on the data subject's financial situation or social status. These include the details of a tenant or a person's professional circumstances, for example.
    3. ***High risk***: Personal data the abuse of which could have a severe impact on the data subject's financial situation or social status. This includes data about health, sensitive personal data and personality profiles.
    4. ***Very high risk*****:** Personal data the abuse of which could put the data subject's life at risk. This includes the addresses of police liaison officers, witnesses in certain criminal cases or persons who are at risk based on their convictions or their religious or political affiliations.

Data file

- Under Swiss law, a ***data file*** is any set of personal data that is structured in such a way that the data is accessible by data subject.

Responsibilities

The following functions are important for any organization that processes personal data:

- The ***Controller of the data file*** is a private person or federal body who/which decides about the purpose and content of the data file.
- The ***Data Protection Officer*** monitors adherence to the data protection policy within an organization and keeps a list of the data files.
- The ***Federal Data Protection and Information Commissioner*** carries out supervision and consulting duties for private persons and federal bodies. In addition, he or she also keeps a register of the data files accessible via the Internet.
- The ***Cantonal Data Protection (and Information) Officer*** performs similar duties at the cantonal level.

Legal foundations

This guide is based on the Federal Act on Data Protection (FADP) – particularly Article 7 – and the Ordinance to the Federal Act on Data Protection (DPO) – especially Articles 8–11 and 20 and 21.

Technical and organizational measures

The risks associated with IT systems can be mitigated by implementing technical and organizational measures. An IT system containing personal data must therefore meet certain criteria to ensure the security of the data.

Technical measures are those that directly involve the IT system. Organizational measures, on the other hand, relate to the system's environment and particularly to the people using it. Only an interplay of both types of measures can prevent data from being destroyed or lost and mistakes, fakes and unauthorized access from occurring. These measures are part of the life cycle of an IT system and must be implemented at every level of the system.

The following diagram (fig. 1) provides an overview of the life cycle of an IT system. It shows how the data is captured, processed, exchanged, stored etc, and at which levels other parties – employees, third data processors or the data subjects – can intervene.

Guide contents

This guide is based on the four main focal points shown in figure 1. It will discuss the technical and organizational measures relating to data access (1), the data life cycle (2), data exchange (3) and the right to information (4).

Each focal point will be presented in light of various aspects and the respective measures associated with it. Some proven practices will be provided for each aspect, as well as tips for developing applications that respect personal privacy. Naturally, the measures will need to be adapted to the individual situation depending on the sensitivity of the data, the nature of data processing to be performed and the scope of the information used.

Finally, existing instruments that help to foresee data protection threats or to formally describe the measures taken will be presented as well.

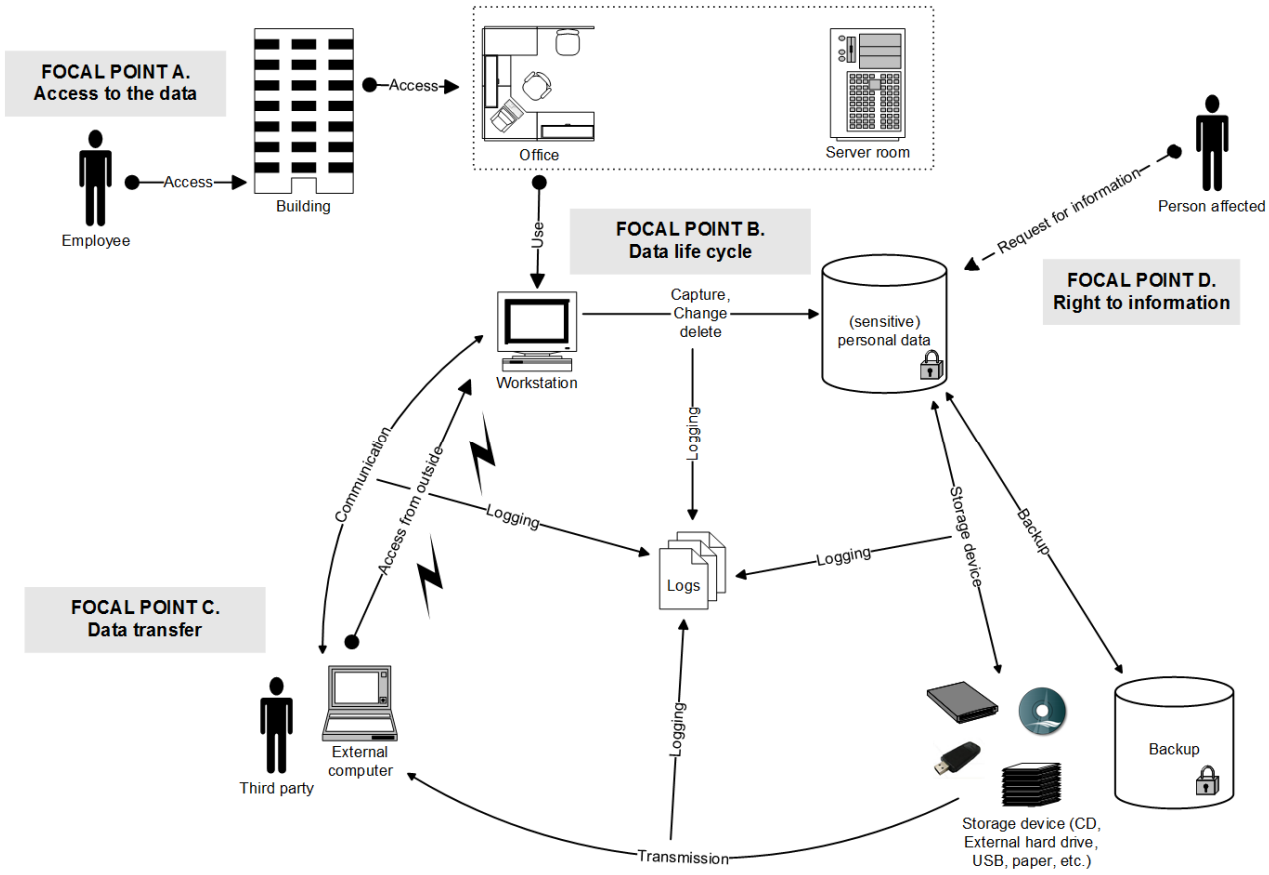


Figure 1. *Overview of technical and organizational measures.*
Each area of the diagram corresponds to one of the focal points in this guide.

FOCAL POINT A. DATA ACCESS

The first thematic area concerns access to the data by the various users. A variety of perspectives apply. For example, the physical location of the data must be assessed thoroughly: where are the data servers located and how can their security be guaranteed while considering all persons involved? Next, it is necessary to define the way in which data can be viewed or changed. This involves a number of different security requirements: the staff computers may only be accessible by persons with access permissions. They must also be protected from all forms of external access. Such attempts to access the system may take place on site – if an unauthorized person walks into the room – or from outside – if an unauthorized person accesses the system via the network. Finally, it is necessary to decide which traces of physical and electronic access to log.

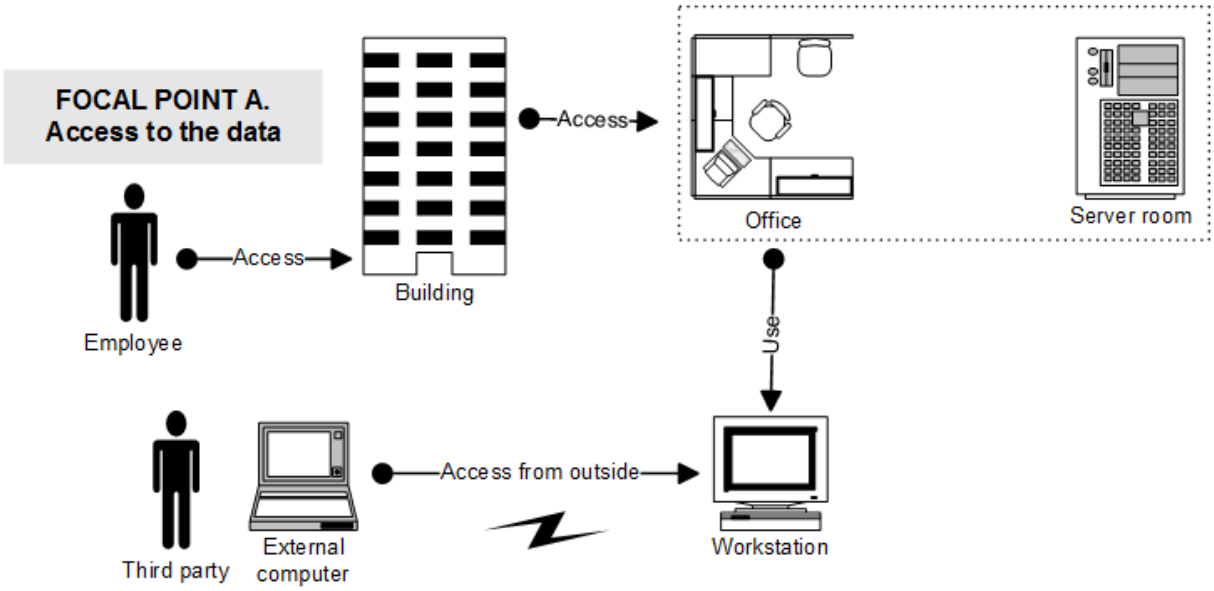


Figure A. *Data access*

The following questions posed in figure A now need to be examined carefully so that specific measures can be recommended.

A.1 How can the premises be secured?
A.2 How can the servers be protected?
A.3 How can the workstations be protected?
A.4 How can it be ensured that the users are identified and authenticated?

A.5 How should access to the user data be protected?
A.6 How can web-based access be monitored?

A.1 Security of premises

The premises include the offices of the persons using the systems who therefore also have access to the data (for data storage in the server rooms see Section A.2). The PCs are the peripheral devices with whom the data can be accessed. Access to these devices must therefore be controlled so that only authorized persons can enter the buildings or offices. These persons may, however, have a broad range of functions that must be taken into consideration when deciding their specific access permissions: This includes the office staff of course but also maintenance and cleaning personnel, etc.

The entire context needs to be considered to ensure that the appropriate measures are implemented. If, for example, several organizations are situated in the same building, they may not all have the same data protection requirements. The security measures may, therefore, need to be adjusted for each floor, for example. The servers may also be kept off-site, with responsibility for their physical safety transferred to other persons; although the client still bears overall responsibility.

Measures

- Controlled access to the buildings. The persons who are permitted to access the building can be authenticated by means of a badge or perhaps an access code.
- A similar arrangement becomes necessary if multiple organizations are in the same building: an electronic access control system can be installed on each floor or for each section of the building occupied by a particular organization.
- Regulate access and reception for visitors in such a way that they cannot freely move around the building on their own.
- Lock the offices outside of office hours.
- Installation of an alarm system that is activated outside office hours in the most sensitive rooms is recommended.

A.2 Server room security

The server rooms are the most vulnerable spaces in an organization because the data is physically stored there. The integrity and availability of the data can only be guaranteed if appropriate measures are taken to ensure that it cannot be lost completely. Here too, the persons who have access need to be defined. The fewer persons who have access, the

better the security. Intentional or unintentional manipulation of the servers that could result in data loss or modification must be prevented. Special measures must therefore be taken to protect the server rooms.

Measures

- Limit the number of persons with access to the server room to as few as possible. Limit the number of technicians who have access to the server room for maintenance purposes. It is also a good idea to have the room cleaned by the same trustworthy cleaning personnel each time.
- Keep a log of all access to the server rooms.
- Install an alarm system that is continuously in operation in order to prevent all forms of unauthorized access.
- The alarm system should also respond automatically to natural events such as fires or floods.
- The server room should ideally be located in the basement because it usually has the fewest doors and windows.

A.3 Workplace security

The employees process the data on their PCs at their workplaces. This work environment must be protected by strategically positioning the various peripheral devices (monitors, printers, etc.). Employees must be provided with adequate lockable storage space.

PCs must be protected with a password that is known to the employee only. Unauthorized access must also be prevented by means of software that can ward off all virus types, malware and attacks of any kind.

Measures

- Set up the workstations in such a way that the monitors cannot be seen from the door so that unauthorized persons cannot see the employees' work.
- Do not leave printed documents lying unattended near the printer. To prevent this, employees may, for example, be required to type in a code on the printer to start a print job.
- Require staff to lock their printed documents and any sensitive objects (flash drives, CD-ROMs, etc.) in lockable cabinets or drawers.
- Keep notebooks and perhaps even desktop PCs chained to the office so that they cannot be stolen.
- Install a virus scanner on each PC and update it regularly.

A.4 Identification and authentication

Identification determines the identity of a person. It is a way of distinguishing the person from everyone else.

Authentication is used to check if a person is really the one they profess to be. There are three ways of doing this: a person can be authenticated by means of an *object* that they carry (e.g. a badge) or a piece of information that they *know* (e.g. a password*)* or a *distinctive characteristic* (a behavioural characteristic such as a signature or a physiological characteristic such as a fingerprint). If at least two of these options are used together, the authentication process is deemed to be strong (e.g. badge and password).

Authentication is required to grant users access to the office space and to the data via their computer. Identification, on the other hand, helps to track who captured, changed or deleted data in the system at which time.

The single sign-on method (SSO) allows users to log into multiple applications in a single authentication process.

Measures

- Make sure that any user accounts that permit authentication are personal, i.e. one user account is used by one person only. This type of account consists of an identifying series of characters (user name) and a password or badge, etc.

- Ideally, each person has multiple user accounts so that they first have to authenticate themselves when they switch on the computer and then again when they use various applications. A person with malicious intent may then be able to access the computer but not the data, because of the protection offered by the application.

- If an SSO login is used, access to the machine also permits access to the applications. The security precautions should therefore be tightened on the SSO systems.

- The password should be strong and changed regularly. A strong password consists of at least eight characters, including upper and lower case letters, digits and special characters.

- The frequency of password changes depends on the password complexity requirements. The more complex the password, the less frequently it needs to be changed, and vice versa.

- Anyone using biometric data for authentication purposes must observe the provisions in the "Leitfaden zu biometrischen Erkennungssystemen" (Guide to biometric recognition systems).[1]

A. 5 Data access

The data is stored on central servers. Most employees do not need access to all the data. Limiting their access to the data they really need reduces the risk of intentional or unintentional mistakes. Data abuse can also be prevented in this way. Access policies and an authorization mechanism must therefore be defined for all staff by job function.

Measures

- Give users differentiated access permissions to the IT system.

- The internal organization should define the access permissions for each employee by means of an access permissions matrix.

[1] http://www.edoeb.admin.ch/ > Topics > Data protection > Biometric data

- Staff should be authenticated each time they switch on their systems. The more sensitive the data they are processing, the higher the authentication requirements should be.

- Keep a log of all access to the system as per the rules in Section B.2.

A.6 Access from outside the organization

There are various ways in which the data could be accessed from outside the organization. Specific protective measures must therefore be taken. For example, an employee may request remote access because he wishes to work off-site and access his office computer from there. This type of access must be systematically regulated in accordance with the organization's policies and the data sensitivity level to permit a secure authentication process. In another example, an authorized third party such as a subsidiary may request access to the data. This case must clearly be addressed with strong authentication. Unauthorized access must be prevented at all costs.

Section C.1 (Network security) contains more in-depth explanations on how to secure communication between external third parties and the organization.

Measures

- Set up secure access for persons who wish or need to access data from outside the organization.

- Use at least two elements for authentication to make it strong.

- Protect personal computers with a firewall.

- Keep a log of all access as set out in Section C.2. (Logging).

FOCAL POINT B. DATA LIFE CYCLE

If the measures listed above are implemented, access to the data can be assumed to be secure, both physically (access to the servers) and in terms of processing (access to the individual workstations). The next objective is to ensure that the data remains secure throughout its entire life cycle. The data must remain intact and reliable from the moment it is fed into the system through all the processing steps until it is either destroyed, anonymized or archived. During this time, it may be processed by authorized persons within the organization or by third-party organizations under contract.
In the course of processing, the data is often loaded onto mobile data storage media such as flash drives, external hard drives etc. It is therefore recommended to log all processing. If problems occur, it will then be easier to trace back to the cause.
All these aspects and situations must be carefully examined in order to prevent improper use.

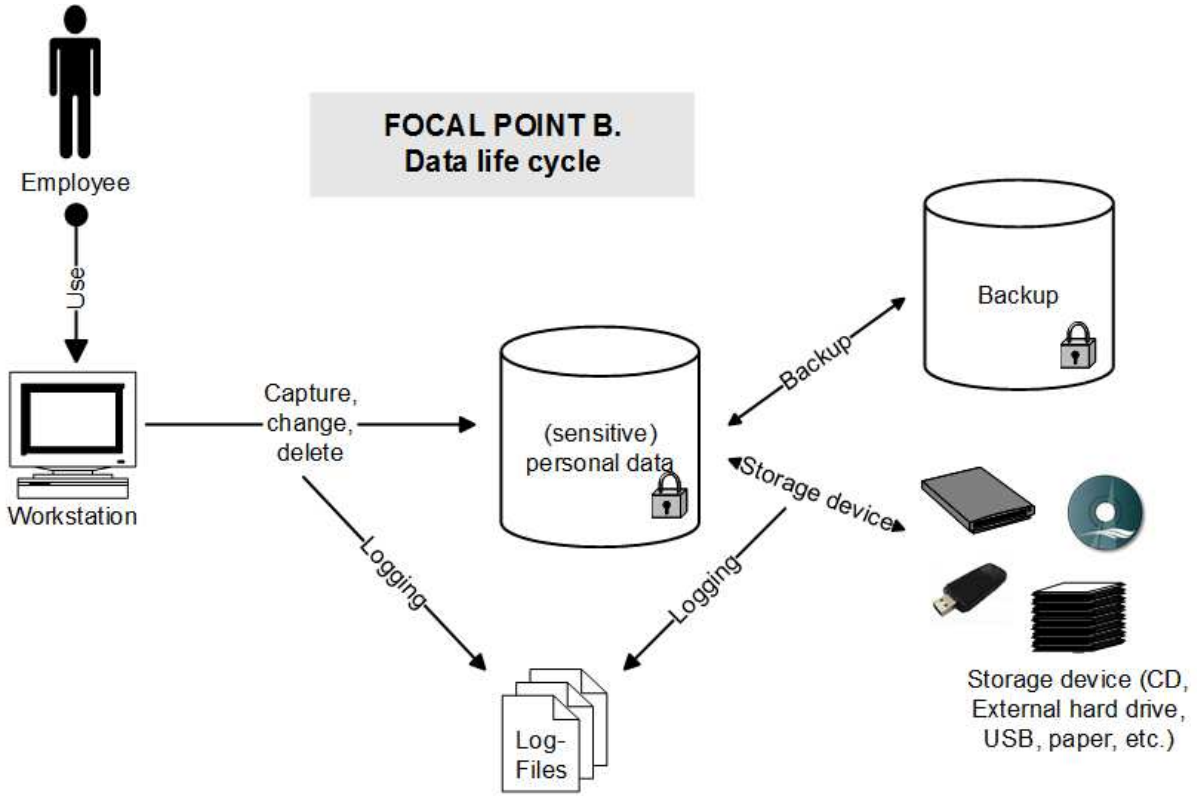


***Figure B**. Data life cycle*

In this focal point we will look at the following questions illustrated in Figure B:

B.1 How should the system data capturing process be organized?
B.2 How should data processing be monitored (monitoring)?
B.3 How should the data be pseudonymized or anonymized?

B.4 How should the data be encrypted?
B.5 How can the various data storage media be kept secure?
B.6 How can the data be stored securely?
B.7 How can the data ultimately be destroyed?
B.8 How is external project work handled?
B.9 How is information security and data protection handled?

B.1 Data input

The first vulnerability is at the point of data capture. It is essential to prevent incomplete or incorrect data from being captured at all costs. During subsequent processing this could result in a misleading picture which, in turn, could result in wrong decisions being made. It is therefore important to develop mechanisms to minimize the risk of errors during data capturing by staff. In addition, a clear distinction must be made between genuine data and test data that is captured by a system during tests.

Measures

- Data is captured by trained and authorized persons only.
- Set up helpful data entry mechanisms in the system. The system detects information gaps and may conduct probability tests on the data captured.
- Use only data that is either fictional or anonymized in tests.
- Data input can be logged as per the rules in Section B.2.

B.2 Logging

It may be very useful to know which manipulations were performed on which data, irrespective of whether it is new data being captured or existing data being changed or deleted. If a problem arises, this type of information can help to determine whether an accident, unauthorized access or unauthorized data processing has taken place. Individual actions can be logged; and all events relating to the IT system are recorded sequentially. The storage period of these log files depends on the sensitivity of the data: the more sensitive they are, the longer they are stored.
The actions that can be logged include data access, input of new data and changes or deletions of existing data. Logging is however only mandatory if especially sensitive data is being processed and the preventative measures to ensure data security are insufficient.

A logging mechanism can also be integrated into the system in other cases. There must, however, be a clear need and a precisely defined purpose for logging. The quantity of information logged and the storage period of the log files must be proportionate.

Measures

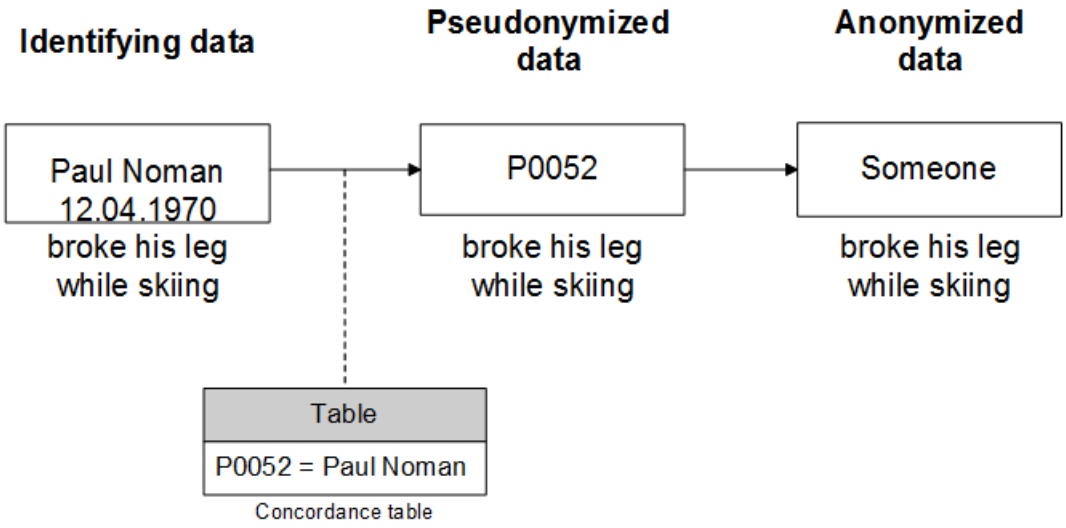
- Create a set of clearly described criteria when setting up a logging mechanism.
- The content and storage duration of the log files should be commensurate to the data and the processing taking place.
- Tell staff that traces will be stored of every action involving the data.
- Keep secure the data files (log files) resulting from the logging process.
- Clearly define the access rights to the log files and limit them to specific functions within the organization.
- Protect the logging mechanism from attacks and unauthorized access that could modify the log contents.

B.3 Pseudonymization and anonymization

To prevent the data subjects in a system from being identifiable, the data can be pseudonymized and anonymized. When data is pseudonymized, all indications allowing a specific person to be identified are replaced by neutral information (pseudonyms). A concordance table defines which pseudonym corresponds to which identifying data. As long as this table exists and is accessible, the pseudonymization process is reversible.

When the data is anonymized, however, the data itself and all options of recreating the original data are eliminated completely. The person can no longer be identified and the process is irreversible. Fully anonymized data is therefore no longer considered personal data.

The following diagram shows this process:



Measures

- If the purpose of the project permits, anonymized data is preferable. Anonymized data is not covered by the Federal Act on Data Protection and most of the measures presented in this guide are not necessary for this kind of data.
- Do not process any indirectly identifying information if the data is pseudonymized or anonymized. Indirectly identifying information results when various pieces of information that would individually be insufficient are combined to allow a person's identity to be concluded.
- If anonymization is not possible, staff should preferably work with pseudonymized data.
- Keep the concordance table secure. It should only be accessible by a limited number of employees. If possible, it should be encrypted.
- If pseudonymization is not possible, staff need to work with personal data. If this data is sensitive, store it in encrypted form (see Section B.4 Encryption).

B.4 Encryption

Personal data is usually stored in the form of a file on a hard drive or in a database. Encryption prevents it from being read or improperly modified. The data is converted into an unrecognizable code by means of a key. It can therefore no longer be deciphered by anyone who does not know the key.
The next focal point (C. Data exchange) discusses problems involving the exchange of data. The associated risks can be reduced through appropriate encryption.

Measures

- Keep the encryption algorithm and, particularly, the length of the key proportionate to the data sensitivity level.
- One data storage medium may contain different data sets encrypted with different keys.
- Keep the encryption keys secure.
- Give only a limited number of employees access to the keys.

B.5 Security of storage media

The data is not only stored on central servers and PCs; many forms of external storage media enable information to be transferred between employees or outside the company without using the network. These storage media also permit data to be stored temporarily.
They may be flash drives, external hard drives or CD-ROMs, for example. Due to their different characteristics, they also serve different functions. For example, flash drives can be overwritten, CD-ROMs cannot. Also, increasing amounts of data fit onto increasingly small storage media. It is important to keep this in mind and not to underestimate the risks associated with these storage media.

Measures

- Provide staff with training in the risks associated with connecting an unknown external storage medium to their PC.
- Encrypt any external storage media that contain sensitive personal data or personality profiles.
- Keep external storage media under lock and key.
- Set up a process for the destruction of storage media. Make the devices necessary for this available.

B.6 Data backup

It is important to protect the integrity and availability of the data on a system. A data backup process must therefore be defined. If a mistake or abusive processing results in data being deleted or damaged, it must be restored to the way it was before the incident. The data backup rhythm must be coordinated with the volume of data processed daily.

Measures

- Define a backup strategy based on the data and its quantity and change frequency.
- Inform staff of the backup strategy.
- Apply the same security measures to the backup servers as to the central servers.
- Make sure that the persons entrusted with restoring data are specially trained in this.

B.7 Data destruction

Personal data should not be stored for an unlimited period. The storage period must be defined, and mechanisms for the final destruction must be planned. Simply deleting the data from the hard drive is not sufficient; it must never again be accessible. The same applies to data on paper or on mobile storage media. The backup copies also need to be destroyed.

Measures

- Destroy data on paper in document shredder.
- Physically destroy CD-ROMs and other mobile storage media as well.
- Physically and irretrievably delete data on rewritable storage media by means of special programs.

B.8 Outsourcing of tasks (processing by third parties)

Organizations often outsource some of their work, e.g. project development, system operation or data backups to third-party companies. The client organization must make sure that the third-party companies follows the same data protection rules as it does. As the client, it is responsible for its own data.

Measures

- The contract with the supplier states that it must adhere to the client's rules.
- As the client, check regularly if the data protection conditions are being observed.
- Regulate the data transfer between client and supplier.

B.9 Security and protection

In order to protect the data optimally, the nature of the personal data (non-sensitive, sensitive or hypersensitive, as per the definitions in the introduction) in accordance with the risk level (low, medium high, very high) must relate to the information classification (INTERNAL, CONFIDENTIAL, SECRET). This allows a matrix to be produced in order to define the protection requirements with respect to the two scales of classification. The least drastic measure applies to all the levels above it.

Data prot. / Info. prot.	non-personal data	non-sensitive personal data	sensitive personal data	hypersensitive personal data
	Risk:	low/medium	high	very high
unclassified information		**protect access**	protect **+ encrypt data** **+ log processing**	protect encrypt log **+ number (*)**
INTERNAL information	**protect access**	protect	protect encrypt log	protect encrypt log number
CONFIDENTIAL information	protect **+ encrypt**	protect encrypt	protect encrypt log	protect encrypt log number
SECRET information	protect encrypt **+ number (*)**	protect encrypt number	protect encrypt log number	protect encrypt log number

(*) The numbering of documents is a measure to protect the information.

Measures

- Develop the system on the basis of the criteria shown in the matrix.
- Implement the appropriate measures based on the matrix.

FOCAL POINT C. DATA EXCHANGE

Today's communication technologies enable people to work online and to exchange information quickly and easily. As a result, data no longer simply stays in the organization but is transmitted outside as well. Exchanges with third parties take place frequently. Data protection must also be ensured during transmission.

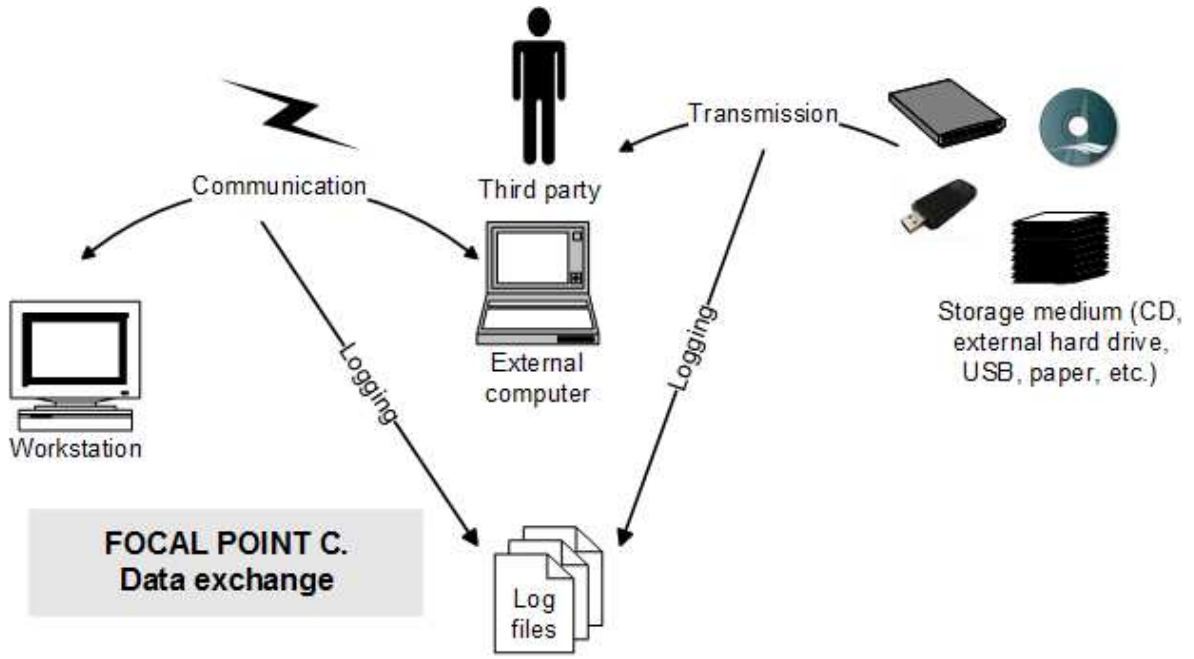


Figure C. *Data exchange*

In this focal point we will look at the following questions illustrated in figure C:

C.1 How can security be guaranteed?
C.2 How does a message that is transmitted to an external third party need to be encrypted?
C.3 How should a message be signed if it is transmitted to an external third party?
C.4 How can mobile data media be passed on securely?
C.5 How are the various information transfers logged?

C.1 Network security

Many data transfers take place on an organization's internal network. So there may be staff who work outside the organization and have access to the intranet or third parties who can access the data. Usually, the data is accessed via the Internet. Security of the network and communications must be ensured. It is essential that secure transmission protocols be used. The TLS protocol (Transport Layer Security), successor of the SSL protocol (Secure Sockets Layer), is an encryption protocol that permits secure data exchanges between client and server. The algorithms and cryptographic keys are negotiated between the client and the server operator. The TLS protocol also permits both parties to be authenticated by means of certificates. This protocol is located at a layer below the usual transmission protocols (HTTP, FTP, etc.). It is transparent to the users, and the application can be displayed as a lock icon in the active window of most browsers.

VPN connections (virtual private networks) also help to secure intranet access. In this type of connection, the encrypted data that is transmitted is encapsulated. VPNs are based on strict cryptographic protocols such as TLS, IPSec or SSTP.

Measures

- Keep data transfers from the intranet to the outside world via the Internet to an absolute minimum.
- Considering using the Transport Layer Security protocol (TLS) depending on the nature of the data that is to be processed.
- If staff or third parties outside the organization access the organization's intranet, a VPN should be set up.

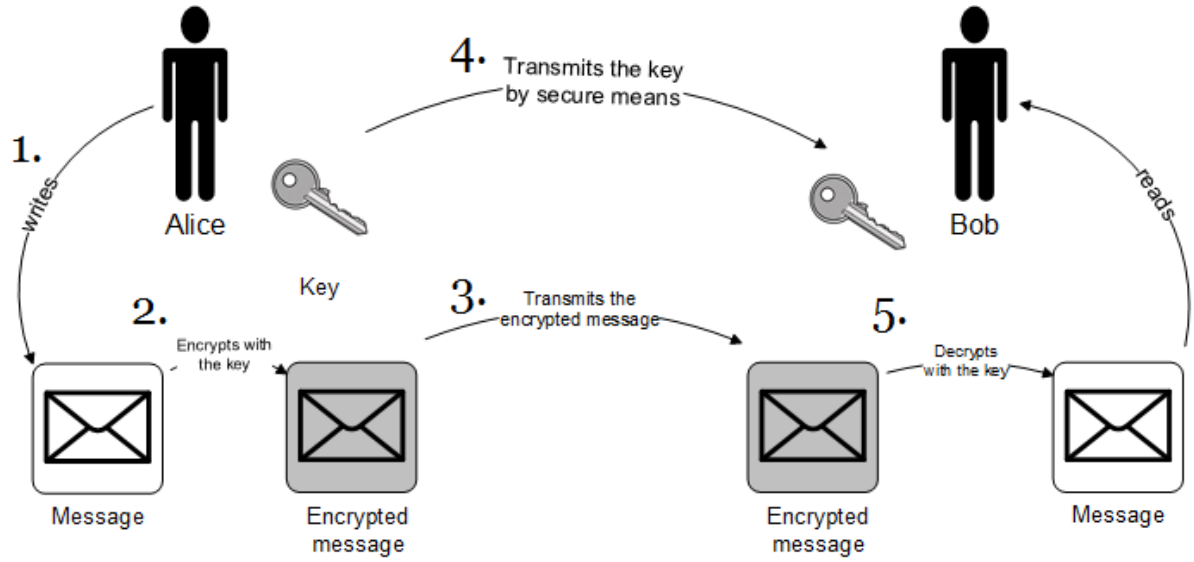
C.2 Message encryption

Apart from the hard drive and the files, it is important to encrypt messages as well. Only in this way can unwanted access to data be avoided in order to prevent unauthorized third parties from reading, changing or deleting a message.

There are two ways in which messages can be encrypted: symmetrical and asymmetrical encryption.

Symmetrical encryption works as shown in the diagram below:

1. Alice writes Bob a message.
2. Alice encrypts the message with a key.
3. Alice transmits the encrypted message to Bob.
4. Alice transmits the key for it to Bob using a secure channel.
5. Bob uses this key to decrypt the message.

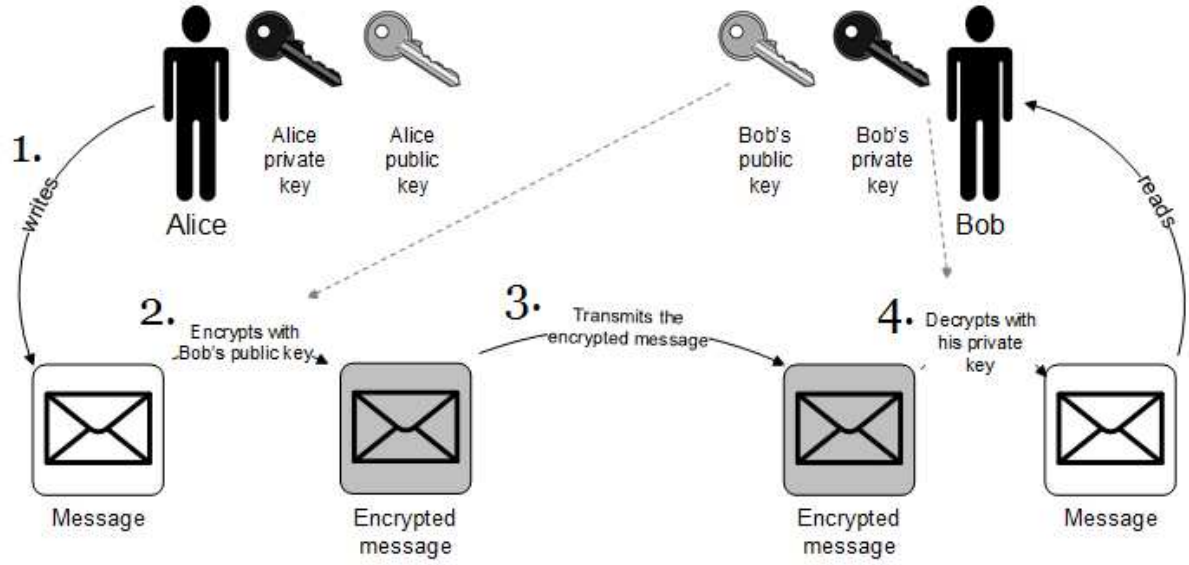


Symmetrical encryption can be implemented easily as it requires only one key. However, care must be taken to transmit the key securely.

Asymmetrical encryption is more complex, however, it addresses the security risk posed by the handover of the key. Instead of a single key, each user generates two keys. One of the keys is public and accessible to everyone and the other one is private, and only the respective person knows it. The public key is used to encrypt the message, the private one is for decrypting it. With this technology, messages can also be signed digitally (see Section C.3 Message signatures).

Here is how the process of asymmetrical encryption works:

1. Alice prepares a message for Bob.
2. Alice uses Bob's public key to encrypt the entire message. This ensures that only Bob can read the message.
3. Alice sends the message to Bob.
4. Bob uses his private key to decrypt the message.



Measures

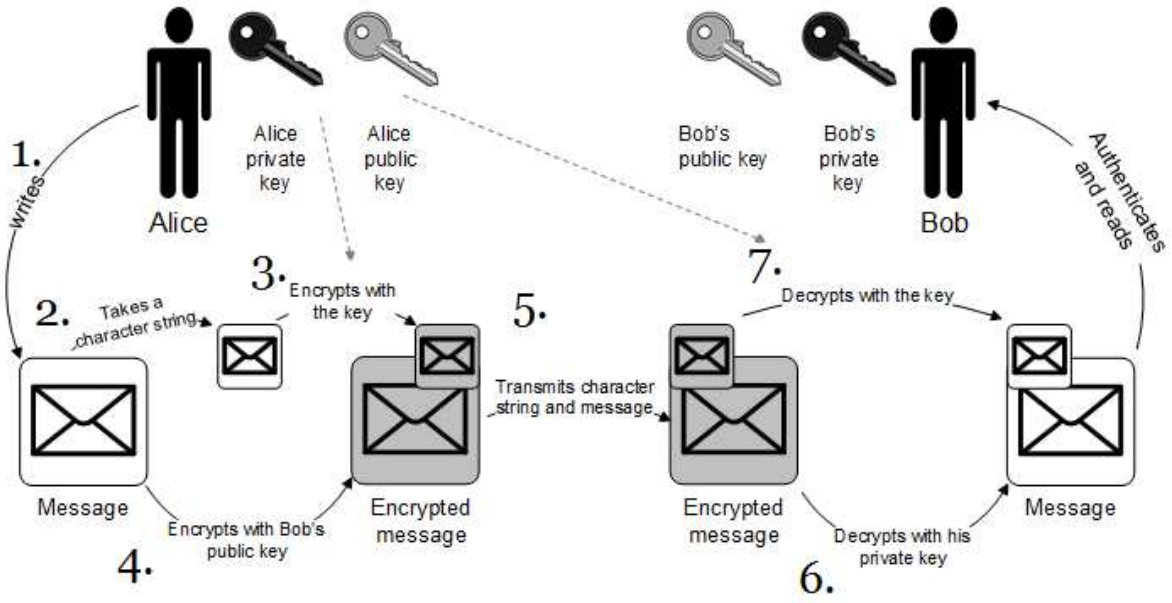
- Determine the most suitable type of encryption. This decision should take into consideration the sensitivity of the data as well as the third parties with which the organization is involved.
- If you choose symmetrical encryption, use a secure protocol for transmitting the key (e-mail, for example, is not secure).
- In the case of asymmetrical encryption, an encryption mechanisms needs to be set up. It is a good idea to link this mechanism to the digital signature function (see Section C.3. Digital signatures on messages).

C.3 Digital signatures on messages

Encrypting a message (see Section C.2 Message encryption) ensures that only the person who has the key necessary for decryption can read the message. It may, however, also be necessary for the message recipient to make sure that the sender really is the person they say they are. With a digital signature on the message, the sender can convey this information securely.

The signature is usually added before encryption. The sequence is as follows:

1. Alice writes a message.
2. Alice takes a series of characters out of the message. This series of characters serves as the signature on the message.
3. Alice signs this series of characters with her private key.
4. Then she encrypts the message as described above.
5. Alice transmits the character string and the message to Bob.
6. Bob decrypts the message.
7. Finally, he compares the character string with Alice's public key to make sure that it was her who sent the message.



Measures

- Make sure that staff are made aware of the situations in which they need to sign and encrypt their information.
- Train staff how to encrypt and sign messages.

C.4 Handovers of storage media

The handover of mobile data storage media is tricky because it means that some of the data physically leaves the organization and is transported to another location. It is essential to protect these storage media during transportation so that the data is not accessible if the media are lost, or worse, stolen. The more sensitive the data on the mobile storage medium, the better the transport needs to be secured.

Measures

- Make sure that the recipients of mobile storage media can be securely authenticated.
- Pack mobile storage media securely before transporting them.
- If necessary, encrypt the mobile storage media.
- Clearly define the transport process. For example, mobile storage media may only be transported in locked suitcases or bags.
- Use the principle of dual control to ensure that data is correctly handed over and received. For example, the giver and the receiver may combine their passwords for access to the data.

C.5 Data exchange logging

The transfer of data via the Internet and the handover of mobile storage media can be logged and recorded in a log. In this way, it is possible to keep track of the sender, the recipient and the handover of the mobile storage medium. In the event of abuse, incorrect use or manipulation, a specific quantity of data can be found again and the route of the data from the handover to the occurrence of the problem can be traced.

The requirements set out in Section B.2 – Logging apply to the logging of data exchanges as well.

Measures

- It is important to describe precisely how the sender and the recipient, the route followed by the data, and all the important points along this route are to be logged.
- Preferably entrust the transfer of mobile storage media to the same employees each time.
- Make sure that the data exchange logs adhere to the principle of proportionality in terms of volume, duration, etc.

FOCAL POINT D. RIGHT TO INFORMATION

The people whose data is on the system are referred to as data subjects. Everyone has the right to know if any personal data about them is being held. If the data exists, the respective person can demand that it be destroyed and, if the data is incorrect, for it to be corrected.

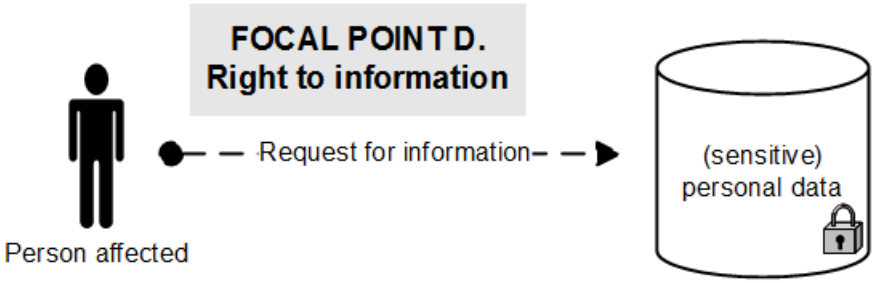


Figure D. Right to information

In this focal point we will look at the following questions illustrated in figure D:

D.1 How can it be ensured that the data subjects can exercise their right to information ?

D.2 How can it be guaranteed that the process to exert the right to information is always followed in the same way (reproducibility of process)?

D.1 Data subjects' rights

The data subjects have a right to be informed about their data. They can request that the data be corrected, blocked or deleted. The organization must be in a position to deal with these requests adequately and to implement them in the system. An efficient mechanism to search for personal data is therefore needed, and it must be possible to conduct these operations successfully. If, for example, a person requests that their data be destroyed, the system must ensure that all the data is actually destroyed.

Measures

- Clear information is available to the data subjects and they are informed of their rights.
- Set up a process for dealing with information requests and announce it to the staff.
- Equip the system with a reliable search mechanism.
- Make sure that the process to change, correct, block or destroy the data is reliable and documented.
- Log every processing action.

D.2 Reproducibility of the processes

The process in which the information requests from data subjects are handled must be clearly defined and reproducible. If the mechanism is coded into the data processing system, all employees can change, block or delete data in the same way. A programmed mechanism is also useful if an inspection is conducted by a regulatory authority because it proves that the right to information can be exercised.

Measures

- Program the functions enabling data subjects to exercise the right to information into the system.
- All staff should use the same procedure.
- If the regulatory authority investigates, it can check the system's built-in procedure.

TOOLS

Some tools to implement the technical and organizational measures already exist.

Evaluation matrix

The Federal Data Protection and Information Commissioner supplies an evaluation matrix for the early detection of data protection risks in which the areas in a project that are vulnerable from a data protection perspective can be identified early in the development process.

The evaluation matrix is available on the website of the EDÖB (go to Data protection - Commerce and economy - Companies).

The data processing policy

The data processing policy is an instrument envisaged by Swiss law and in which the appropriate technical and organizational measures are defined. The aim of the policy is to ensure the necessary transparency in the development and administration of a personal data file. It summarizes and centralizes the documents and information produced by the various units conducting the project. It therefore provides the system operators and those in charge of data protection with a complete set of documentation which enables them to look up and apply proven practices.

The data processing policy must be written by the controller of the data file.

Policy contents

If the controller of the data file is an individual, the processing policy must contain a description of the internal organization and the data processing and monitoring processes and also fully document the planning, development and operation of the IT resources, i.e. the software and hardware.

If the controller of the data file is a Federal body, a data processing policy is only required if that file (1) contains sensitive data or personality profiles, (2) is used by multiple Federal bodies, (3) is accessible to third parties such as cantons, foreign authorities, international organizations or private persons or (4) is linked to other files.

The contents of the processing policy for Federal bodies are very precisely defined:

1. The internal organization, i.e. the operations performed by the system and the organizational structure, must be documented. In particular, the various responsibilities (data protection, controller of data file, etc.) must be listed.

2. The documents on the planning, implementation and operation of the IT resources must be transparently structured.
3. An overview of the technical and organizational measures shows which ones have already been taken.
4. The origins and processing purpose of the data must be described.
5. The reporting obligation is described with all the required information.
6. All data fields are defined. An access matrix shows the organizational units and persons who have access to the data.
7. The measures to facilitate the right to information are defined.
8. The configuration of the IT resources lists all the software and hardware used.

The processing policy must be updated regularly and made available to other bodies involved.

The document “What must a processing policy contain” by the FDPIC may be useful when writing the processing policy [2].

CONCLUDING REMARKS

The measures set out in this guide provide adequate data protection. However, other factors, such as the global environment and sensitivity of a specific project or the quantity of required data must always be taken into consideration as well.

The controller of the data file is responsible for data protection. The earlier this topic is addressed when a project is developed, the better the associated risks can be mitigated.

[2] http://www.edoeb.admin.ch/ > Documentation > Data Protection > Guides > Technical and Organizational Measures