Data Protection Concept
top itservices AG

This data protection concept explains the technical and organisational implementation of data protection measures in companies.

It has been compiled as an information service for interested persons.

15.10.2020
Version 1.3

top itservices

Table of Contents

In the text, for the sake of better legibility, there is no explicit differentiation between the female, male and other forms; nevertheless all are meant.

1 Data Protection Policy

We consider the protection of personal data by our company, in particular the protection of the confidentiality, integrity and availability of your data, as being our duty which is regularly monitored by the executive board, the data protection officer and other persons at top itservices AG.

The executive board is aware of the utmost importance of data security and its personal responsibility. By introducing, implementing and continuously improving our data protection management system we want to highlight the importance which the processing of personal data has for us.

1.1 Basic principles

We place priority in implementing the minimum measures for meeting our legal requirements.

All measures are based on whether their objective can be achieved with a proportional use of resources. The goal is always to adequately master the risks associated with data processing, preferably without interfering with the legitimate interests of the company any more than is absolutely necessary.

The following principles apply to the processing of personal data:

We will only process personal data if and for as long as we have a clear mandate or for as long as the corresponding obligation exists!

The respectively pursued purpose for processing data and the associated legal basis are documented in the directory of processing activities. Data may not be processed for purposes which are not featured in this document!

We will avoid using personal data wherever possible!

We only use data needed to achieve legitimate objectives. We will not process data which is not required for a specific purpose.

Insofar as an objective can also be achieved using anonymous or pseudonymous data, the use of such data will be preferred. General and generalised information will be processed in preference to the processing of detailed information.

The time period during which your data will be processed must also be limited to what is absolutely necessary. While complying with the duty to preserve records, data will be deleted as early as possible.

We will protect the interests of the persons concerned!

Data will only be processed while accounting for the interests and expectations of the person concerned. Personal data will only be used insofar as this cannot be avoided to achieve a legitimate objective and insofar as this is reasonable for the person concerned.

We will ensure that those concerned understand how their data is being processed by us, and we will protect the rights of the persons concerned, in particular their right to information.

We will restrict access to personal data!

We will treat all personal data in strict confidence! Data will only be made available to individuals or for processing purposes insofar and for as long as this is necessary in individual cases. This restriction also applies generally to the collection of data as well as to the information contained in the data.

We will ensure the accuracy of the personal data we process!

We will immediately correct any inaccurate data that comes to our attention.

We will ensure the security of the data we process!

Our state-of-the-art technical and organisational measures are designed to ensure an adequate protection against any breaches of privacy. Here we will account for the risks associated with the processing of data.

Our data protection measures are verifiable!

We will assess and measure the success of our data protection measures to a reasonable extent, whereby we will correct any undesirable developments.

1.2 Responsibility and tasks

Although the board possesses the overall legal responsibility for protecting data, it cannot actually complete this task by itself. This requires that the board sets up a suitable organisation and assigns related tasks, whereby the board will remain personally responsible for the correct selection and supervision of the appointed staff.

The board can only meet its remaining responsibility when it is being adequately informed. This is why a corresponding reporting system has been introduced. This system allows all persons in charge to report direct to the board.

As a matter of principle, all our staff are called upon to actively support the company's data protection measures and to ensure that these are being correctly implemented in their area of responsibility. All staff are being trained accordingly and will be continually reminded of the importance of data security. Staff members are being adequately instructed. In this manner all staff members are personally responsible.

Responsibility has been clearly delegated to all areas and tasks. Responsibility will always be clearly delegated to a specific person whereby this person will also be designated through his function or position. Insofar as this is necessary, a suitable deputy will be appointed. Deputies can also be several people or members assigned a role. It will always be ensured that the person in charge and any representatives will be both professionally as well as technically able to fulfil their tasks carefully, confidently and adequately.

Conflicts of interest must be prevented when responsibilities have been delegated. Incompatible roles have been clearly identified and documented.

The responsibilities in the company are being documented on a continuous basis.

To ensure that relevant interests are also being accounted for across departments, concepts shall be established by defining the roles, positions and people who should possibly be involved or informed.

The following positions have been entrusted with special tasks in the field of data protection:

- **Data Protection Officer:** The data protection officer informs and advises the company's staff about their data protection duties. He monitors the compliance with the data protection regulations. The officer is unconstrained by directives and not directly responsible for the correct application of the data protection regulations. The obligation to appoint a data protection officer is based on relevant legislation.
- **Head of Data Protection:** The executive board is at all times legally responsible for the company's compliance with data protection regulations. The board has decided to delegate this joint responsibility to an individual board member. The implementation of the measures adopted by the board can also be delegated to other persons.

- **Data Protection Coordinator:** The data protection coordinator ensures that the data protection measures are carried out in the individual departments of the company and, if necessary, he acts as the contact person between these departments. The coordinator has the necessary power to direct within the scope of the data protection regulations. The coordinator reports to the executive board on a regular basis.

2 Data Protection Officer

Contact to the data protection officer:

By post:

Datenschutzbeauftragter der top itservices AG

c/o activeMind AG

Potsdamer Str. 3

80802 München

E-Mail: datenschutz@top-itservices.com

Tel.: +49 (0)89 / 91 92 94 900

3 Technical and Organisational Measures

The following contains a description of the technical and organisational measures that have been taken to ensure data protection and data security. The objective is to especially ensure the confidentiality, integrity and availability of the data and information being processed by the company. The measures comply with the internationally recognised DIN ISO/IEC 27002 standard.

3.1 Policy

The data protection policy of top itservices AG contains the board's mission statement concerning the handling of personal data by the company. All staff, freelance collaborators and subcontractors are obliged to abide by these basic principles.

The IT security level achieved by the organisational units and the procedures and systems will be monitored through periodic audits and continuous controls.

Daily operations will be monitored in cooperation with the security officer.

The security policy will be reviewed at least once a year insofar as an essential change does not necessitate an earlier review. This will help to ensure the ongoing appropriateness, suitability and efficiency of the regulation.

The security officer is the person in charge of the security policy. He is responsible for developing, reviewing and checking the policy.

3.2 Organising the information security

Senior staff at top itservices AG is responsible for the complete implementation of the principles of IT security and for fulfilling the assigned IT security tasks in their organisational unit.

Information security roles and responsibilities are defined in the IT security organisation. Conflicting and incompatible tasks and responsibilities have been separated to reduce the possibility of unauthorised or unintentional changes or a misuse of the values (e.g. operating supplies, removable media, notebooks) of our company.

We possess a procedure which establishes when and by whom relevant authorities shall be notified and recognised data protection and information security incidents reported in time.

We are also in regular contact with special interest groups allowing us to remain informed about changes and improvements in the field of data protection and information security.

In projects for which we are responsible data protection and data security is an element during all stages of our project plan.

With the help of our respective guidelines and procedures for using mobile devices, we also ensure that data is protected and secure in these areas.

3.3 Staff security

Our staff have been carefully selected and scrutinised for their suitability for their positions in our company. We have codified their responsibilities in job descriptions, and we regularly review this compliance with our staff. Before beginning their job all employees sign a confidentiality and data protection agreement which applies beyond the termination of their employment relationship. Our staff are trained in the fields of data protection and data security, whereby knowledge in this field is brushed up when staff change their function. Our staff are therefore aware of their responsibility in this regard.

In a documented process for the time before, during and after the termination of an employment relationship, we ensure that personal data are protected and data security is ensured. This also includes disciplinary measures in the event of a breach of data protection rules.

3.4 Administrating the values

We inventory and maintain all values (such as operating supplies, removable media, notebooks) and information carriers that are associated with personal data.

We have appointed persons responsible for protecting these values who are responsible for the life cycle of a value.

Documented rules have been established for a permissible use of these values. Their return is documented.

Our information and data are classified and designated as required by law and their value, their criticality and their sensitivity protected against unauthorised disclosure or alterations.

Corresponding with this classification scheme we have developed and implemented documented procedures for handling our values, in particular also for dealing with our removable media. We possess a documented and regulated procedure for transporting data carriers to protect them from unauthorised access, misuse or falsification.

We safely dispose of data carriers which are no longer needed while using a documented procedure and committed and certified service providers.

3.5 Access control

We have regulated and documented measures which assure that authorised persons only have access to those personal data for which they possess an inspection and processing right.

Authority to access IT systems will be endowed in a regulated process on the basis of a documented and restrictive authorisation concept. We have regulated and implemented access to networks and network services.

We have ensured that only authorised users will have access to systems and services and that unauthorised access is prevented, in particular through a formal process for registering and deregistering users which allows access rights to be correctly assigned.
The administrative rights we grant are restricted and controlled.
We possess a documented and regulated procedure for handling passwords.
The normative and actual condition of user access rights are reviewed on a regular basis. If required they are revoked or adjusted accordingly.

We restrict access to our data on a needs basis and control access to our systems and applications through a secure registration process. We use a system featuring secure and strong passwords. The use of auxiliary programs which could bypass our system and protective application measures is restricted and tightly controlled.

3.6 Cryptography

An adequate and effective use of cryptography ensures the securing of confidentiality, authenticity and integrity of information. This is why we have implemented a regulation concerning the use of

cryptographic measures by the company which also includes the administration of cryptographic keys and which meets security requirements.

3.7 Physical and environmental security

We have taken documented and regulated measures designed to prevent unauthorised persons from accessing the equipment used to process data and use personal data. These measures include but are not limited to the following factors:

- The business premises are situated in different office buildings which are used exclusively.
- The entrances are controlled.
- The doors to security areas are always kept closed. Security is ensured through a token/security key system.
- Visitors and external service providers are admitted individually with name and contact person being documented.
- Fire protection regulations are observed.
- Security zones with access restricted to authorised personnel exist.
- IT rooms are closed separately and can only be opened by authorised staff.
- Utility installations are protected against power failures and disturbances.
- The safety of the cable system is ensured.
- Systems are maintained according to a plan which is put into practice.
- Changes to systems and information and their removal are carried out systematically.
- The security of systems outside of the business premises is accounted for.
- Resources are disposed of or reused according to plan.
- User equipment is secured through a coded system.
- Clean Desk and screen lock guidelines are followed.

3.8 Operating security

We possess regulated and documented measures to ensure a proper and secure operation of information and data processing equipment. These include control measures for changes to the information processing equipment as well as a control and regular measurement of our capacities and resources to ensure the availability of the required system performance. For example, in this manner the following values among other things are being currently monitored on a regular basis:

- Hard drive status and available memory
- Raid status
- Services and status of all virtual equipment
- Storage occupancy of the storages and central memory
- Use of ether net in Kbit/s and Mbit/s
- Number of RDP sessions of the individual terminal servers
- Throughput and use of the Firewall
- Availability of all servers through VPN

- Availability and throughput of the switches
- Availability of the mail services (internal and external)

We have implemented and documented a protected procedure for data security.

Standard maintenance windows have been defined. Additionally required windows will be announced at least three days in advance.

It is essential that development, test and operating environments are kept separate at our company allowing us to focus on the maintenance of this separation.

To protect against malicious software, recognition, prevention and recovery measures have been taken and are being updated regularly.

We possess a centrally monitored and secured event logging system, and for storing sensitive personal data we have adopted measures to protect the private sphere. All recording facilities and protocol information, including administrators and operator protocols, are protected against manipulation and unauthorised access.

Our clocks are synchronised centrally using a single referential time source.

We use a centralised procedure to control the installation of software on systems at our company.

We possess centrally implemented regulations for limiting software installations.

For audits to our information systems we have established measures designed to keep the disturbances of our business processes at a minimum.

3.9 Communication security

The security of the personal data and information stored on our networks and network services is absolutely essential. That is why we are using documented measures which administrate, control and secure our networks.

On a needs basis information services, users and information systems are being kept as far as possibly separate from each other.

We possess regulations and procedures for transmitting information and data and transferring agreements regulating the transmission of information to outside authorities.
Our electronic communication is adequately secured. We have implemented measures for securing our communication including securing it from unauthorised access, from changes or from a denial-of-service attack which correspond with the classification scheme taken over from the organisation.

To protect our data, we enter into confidentiality or secrecy agreements that meet our needs and which we review on a regular basis.

3.10 Acquisition, development and maintenance of systems

We have ensured that data and information security remains an integral part of our systems throughout their whole lifecycle. This also includes the demands place on and the securing of information systems which provide services through public networks. Transactions with application services are secured on a needs basis. We have also established a method for administrating system changes to

ensure the integrity of the system and its application as well as of the products from the early design stages through to the subsequent maintenance work. With changes to operating platforms, applications critical to business are checked and tested to ensure that there are no negative effects on the organisational security. We possess a controlled method for analysing, developing and maintaining secure IT systems.

3.11 Supplier relations

We carefully select our suppliers during the preliminary stages and check their suitability with regard to the safeguarding of data and information security.

Documented arrangements (agreements for commissioned data processing) secure the protection and secrecy of our values and data. Suppliers are being committed to implement technical and organisational measures to ensure their conformity with these arrangements.

A regulated and user-defined access authorisation procedure exists for values and data that the respective suppliers stringently require.

To ensure a secure supply chain, suppliers may only commission sub-suppliers with our approval.

We regularly check the data protection and data security measures of our suppliers in order to maintain the arranged protection level. The assigned authorities are also subject to a continuous documented control.

After terminating the supplier relationship, these suppliers are obliged to return all data and values to us or to destroy them properly. In addition, the duty to observe the secrecy obligation remains indefinitely.

3.12 Handling information security and data protection incidents

Our company possesses a regulated documented process for handling information security and data protection incidents in order to ensure a consistent and effective strategy in this regard. Staff are called upon to immediately report any data protection and security incidents, and they are also being trained regularly in this aspect.
All incidents are documented, classified and evaluated. A special intervention team has specific instructions on how to deal with such an event.
Together with the board improvement measures resulting from the knowledge gained and the collected evidence relating to an event are regularly discussed and implemented.

3.13 Information security aspects with Business Continuity Management

The availability of a system allowed within the limits of information security is specifically assessed and documented. We derive the technical and organisational specifications such as redundant systems and connections or feasible plans from the requirements and implement them accordingly. A comprehensive contingency plan provides the framework for the corresponding instructions for selected documented emergency scenarios. Continually updated training plans for the implemented measures and the documentation of the application of corresponding tests round off the contingency management process. All server and storage systems are equipped with a manufacturer’s warranty of at least 36 months, usually however 60 months.

3.14 Compliance

We have documented all relevant statutory, regulatory, self-imposed and contractual requirements as well as the procedures of our company for complying with these requirements, and these are kept up to date by us.

We have also implemented appropriate procedures with which the compliance with the statutory, regulatory and contractual requirements concerning intellectual property rights and the use of software products protected by copyright is ensured.

Our recordings and personal data are secured on a needs basis according to the statutory, regulatory, contractual and business requirements. Yearly activity reports from the data protection official document the measures that have been taken.

For this purpose we comply with the regulations of cryptographic measures.

To ensure the protection of our information and data a regular independent review of our information security and data protection level, our security and data protection regulations as well as the adherence to technical specifications is carried out.

4 Additional Measures

4.1 Directory of procedures

Current processing overviews and procedure directories exist.

4.2 Data impact assessments

Insofar as this is legally required, before being implemented procedures will be identified on the basis of predefined risk criteria and stages and subsequently compared with protection measures. The assessments arrived at in terms of data protection legislation are incorporated in the implementation of the measures and also documented.

4.3 Training and sensitising staff

Staff are regularly trained and sensitised in matters concerning data protection with these measures being documented accordingly.

5 Regulations in the company

The information security and data protection regulations existing in the company include the following:

- Policy regarding the rights of persons concerned
- Data protection management system handbook
- Policy on risk analysis and response
- Onboarding staff
- Offboarding staff
- Order processing policy
- Policy regarding the assignment of rights
- Data protection contingency policy
- Data archiving and deletion policy
- IT use policy

- Contact persons in case of data protection emergencies
- Overview of data classification and processing

6 Release

This rule will be released when it is published in topNet.

Version	released	Changes
1.0	03/2018	First version
1.1	04/2018	Adjustments
1.2	07/2020	Adjustments
1.3	10/2020	Adjustments

7 Scope

This rule applies to the entire company.