Annex 1 –Technical and organisational measures taken by simple system

article 32 General Data Protection Regulation, Version 1.0

Table of contents

Amendment chronology

Version	Date	Prepared by	Amendment
1.0	21.12.2017	DSB	Initial issue

1. Introduction and overall conditions

The following principles represent the data protection concept implemented by simple system GmbH & Co. KG (hereafter simple system).

simple system thereby establishes the standards according to which the branches handle and protect all forms of paper-bound and electronic information during processing from the time the data is received to its destruction and also destroy the data after the service has been provided in accordance with the particular requirements agreed with the customer.

The relevant measures that simple system carries out in order to prevent unauthorised handing of personal data and documents as well as the unauthorised use of personal data in accordance with the applicable data protection laws and to ensure appropriate IT security will be described in individual sub-sections.

1.1. Area of application

The following principles will be complied with throughout processing and therefore on all assignments and functions assumed by simple system.

Since it is to be assumed on the basis of the highly varied assignment specifications that different jobs with higher or lower data protection standards will have to be processed, the area covered by the standards defined in this document will be limited or extended through appropriate individual agreements with the clients. This may be the case particularly if sub-contractors are involved in providing the service.

Moreover, security specifications may be increased at the client's request provided that this is agreed in writing in a document specifying the relevant documentation in the assignment.

1.2. Responsibilities and overall responsibility

1.2.1.1. Overall responsibility

Overall responsibility, particularly as regards the establishment of requirements as well as the contents and objectives of the data security concept including the permanent checks on and improvement in regulations will be assumed by simple system's coordinator for data protection. This will support the data protection officer in a supervisory and advisory capacity.

1.2.1.2. Monitoring and implementation

An external data protection coordinator, who exercises his functions in accordance with the provisions of the relevant data protection law, is appointed in order to supervise implementation. The following is appointed as data protection coordinator:

Company	Address	Contact
MKM Datenschutz GmbH	Äußere Sulzbacher Straße 124a	+49 911 66 95 77 55

The data protection coordinator of the simple system supports the data protection officer in the fulfilment of its functions.

2. Technical and organisational measures

2.1. Confidentiality (article 32 para. 1.b General Data Protection Regulation (hereafter DS-GVO))

2.1.1. Access control

The objective of access control is to prevent access by unauthorised persons (e.g. to data processing installations) enabling the processing or use of personal data. The concept of access is to be understood as relating to area.

We ensure access to our company premises by the following measures:

- Recorded issue of access permits
- Withdrawal of access permit on leaving the company
- Door locking devices (electronic door opener) with chip card

2.1.2. Admission control

The purpose of admission control is, with the aid of suitable measures, to prevent unauthorised persons from penetrating or using data equipment installations and systems on which personal data is processed or used.

We have implemented the following measures in order to protect admission to our network:

- Management of users through registration
- Individual user name and password
- Segmentation of networks in accordance with degree of protection required
- Use of virus scanner and firewall
- Use of secure transmission technology (VPN)
- Password regulations (number of characters, special characters, chronology, no consecutive characters)

2.1.3. Identity control

The aim of input control is to ensure that only those entitled to use data processing systems can access personal data that is subject to their access entitlement and that personal data cannot be read, duplicated, amended or deleted by those unauthorised during processing and use of such data and after it has been stored.

We have taken the following measures in order to prevent unauthorised activities within simple system's systems apart from those allowed by entitlements:

- Issue of rights in accordance with roles / organisational units
- Management of access rights by the administrator
- Disposal of data media and paper in compliance with data protection
- Mobile data media do not contain any personal data

2.1.4. Separation control

The aim of Separation control is to ensure that data collected for different purposes is also processed separately from each other.

We have implemented the following measures in order to ensure that data collected for different purposes is also processed separately from each other:

- Separation of functions through systems that have multi-client capability
- Creation of an entitlement concept and allocation of roles
- Data separation through network segmentation
- Separation of development, test and operative systems

2.1.5. Use of pseudonyms (article 32 para. 1.a DS-GVO; article 25 para 1 DS-GVO)

The processing of personal data such that data can no longer be attributed to a specific persona concerned without the addition of complementary information, provided that this complementary information is stored separately and subject to appropriate technical and organisational measures

- Use of pseudonyms through a unique identification number (ID). This ID is used in the system through the creation of logging systems.

2.2. Integrity (article 32 para. 1.b DS-GVO)

2.2.1. Transfer control

The aim of transfer control is to ensure that in transferring personal data electronically or whilst such data is being transported or stored on data media, it cannot be read, duplicated, amended or removed by those not authorised and it it is possible to verify and also determine at which points the transfer of personal data by means of data transmission installations is planned.

We have implemented the following measures with regard to the transfer of personal data:

- Secure installation of servers and SAN (security area) / NAS
- Company-owned domain for e-mail communications (internal)
- Transfer to third parties only after the legal basis has been checked
- Written record of transfer to third countries
- Secure transfer of data shipments (SFTP, VPN)
- Restriction of the group of individuals entitled to transfer

2.2.2. Input control

The aim of input control is to enable subsequent identification as to whether personal data has been entered in, amended or deleted in data processing systems and equipment and by whom.

We ensure traceability within data management as follows:

- Logging the input of personal data
- Determining the purpose of data logged

2.3. Availability and resilience (article 32 para. 1.b DS-GVO)

2.3.1. Control on availability

The aim of availability control is to ensure that personal data is protected from destruction or loss, both physically as well as logically.

Since the data is only processed on the premises of our external data centres, we refer to attachment A of this agreement dealing with the availability of data.

2.4. Procedure for regular monitoring, appraisal and evaluation (article 32 para. 1.d DS-GVO; article 25 para. 1 DS-GVO)

2.4.1. General

General procedure for regular monitoring, appraisal and evaluation

- Data protection management
- Incident response management
- Regular checks by the data protection coordinator

2.4.2. Job control

The aim of job control within the meaning of article 28 DS-GVO is to ensure that personal data processed as part of a job can only be processed in accordance with the client's assignment and instructions.

- Contractual provisions in accordance with § 11 BDSG (job data processing)
- Sub-contracting only where an equivalent level of protection is ensured
- Verification and documentation of measures taken by the service provider
- Commitment of service providers' employees to secrecy

3. Documents accompanying the technical-organisational measures

Personal data is processed on servers in data centres appointed by simple system. simple system has concluded all the necessary data protection contracts with the data centres. The technical and organisational measures implemented by the data centres are described in attachment A.

4. Additional measures

All simple system employees who process personal data have signed a written commitment to the safeguarding of confidentiality. Employees receive regular training from the data protection coordinator in handling personal data.

5. Concluding provision

Data protection is subject to a continuous improvement process at simple system and is adapted in accordance with current and applicable rules governing data protection. The document is regularly updated.

Annex 1.A - Technical and organisational measures implemented by the data centre service provider

Technical and organisational measures implemented by the data centre service provider (SpaceNet AG)

1. Access control

- Electronic access control with logging
- Documented issue of keys to employees
- Guidelines on accompaniment to visitors to the building
- 24/7 manning of data centres
- Video surveillance at all entrances and exits
- Door locking devices (electronic door openers etc.) with chip card or finger-print scanner
- Admission only after registration with visitor control, accompaniment and induction
- Video surveillance of all data centre access areas and rooms
- Alarm system for external security (doors, window opening contacts)

2. Admission control

- Admission is protected by password, admission only to the service provider's employees and, under certain circumstances, to client's employees
- Passwords issued by service provider to the client are issued by password generator
- Central and protected identity management
- Identity control guideline

3. Identity control

- Service provider ensures the prevention of unauthorised admission by means of regular security updates and backups (in accordance with the latest state of technology)

- Audit-secure and binding entitlement issue procedure for the service provider’s employees
- The client has sole responsibility for data/software/applications with regard to security and updates
- Demand-oriented design of entitlement concept and access rights together with the client as well as its monitoring and logging
- Logging of jobs via ticket system
- Automatic generation of log files wherever technically feasible and sensible as well as the evaluation of these logs in suspicious circumstances. Cyclical automatic deletion by rotation
- Authentication procedure
- People to contact and their entitlement are stored individually

4. Transfer control

- All employees are bound to data secrecy in accordance with § 5 of the German Data Protection Law (BDSG)
- Data protection compliant deletion of data following completion of job in accordance with section 10 of the agreement
- Opportunities for encoded data transmission are provided to the extent of the service described in the main order
- Separation of networks, particularly between the Internet (outside world) and internal network. Implementation of multi-tier architectures with graded security areas and protective measures (e.g. firewalls, intrusion detection systems etc.) are possible
- Encoding and tunnel links (SSL, VPN)
- Logging of transfer transactions

5. Input control

- Data is entered and recorded by the client itself.
- External access logged
- Proof of job ordered and of its completion in the ticket system

6. Job control

- Our employees are instructed in data protection law at regular intervals, also with regard to the client's right to issue instructions
- The service provider has appointed an operating data protection coordinator and ensures that he is adequately and effectively integrated into the relevant operating processes through the data protection organisation

7. Availability control

- Backup and recovery concept with daily data backup depending on services ordered as part of main order
- Use of fixed-disk mirroring
- Use of uninterrupted electricity supply
- Use of port regulations
- Avoidance of single-point-of-failures as a basic concept in all the infrastructure in data centre operations, i.e. availability ensured through system and component redundancy
- Avoidance of single-point-of-failures in client systems depending on services ordered as part of main order
- Redundant electricity supply (main supply, transformer, uninterrupted electricity supply by means of USV, emergency generators based on external diesel motors)
- Backup, also shared backup, can be reserved for separate locations
- Use of firewalls and load balancers in order to filter admissions and contents and horizontal load balancing can also be reserved with shared services
- Air conditioning
- 7x24h monitoring of systems in the data centre infrastructure.
- Emergency plans (BCM) in accordance with ISO 27001-Standard for Data Centre Operation

Technical and organisational measures implemented by the data service centre Noris Networks

1) Access control

Data requiring protection is processed in the noris network data centre.

Avoidance of indications of parts of the building requiring protection

The data centres are to be regarded as parts of the building requiring protection. There is no indication of the exact location of the area covered by the data centre and the associated technical facilities at these places.

Locked doors and windows

The data centres do not have any windows; doors lock automatically.
The external entrance (on the perimeter) to the data centre (to the control channel) in the NBG3 data centre in the Deutscherrnstraße in Nürnberg is accessible during the day but there is no indication whatsoever that a data centre is located here (through the use of everyday characteristics) and the external door to the control channel is then already locked again; not until the control channel is there any visible identification as a data centre. Nor is the overall external appearance of the Deutschherrn Block identifiable as the location of a data centre although many different data centres have their premises here.

The external door (on the perimeter) and the basement garage to the MUC6 data centre in the Seidlstraße in Munich are accessible during the day but there is no indication whatsoever that a data centre is located here (through the use of everyday characteristics), the external door on the level leading to the porter's office is then already locked gain; there is no indication that a data centre is located here until the premises are actually entered.

Records

The control logs of entry through the door are viewed, checked on a spot check basis and archived.

Office premises

Access control systems at the entrances. No prominent ground floor location (with the exception of the branch in the Deutschherrnstraße in Nürnberg where short walking distances to both the NBG3 and NBG4 data centres are important). Employees are instructed to close doors and windows outside office hours and to keep them locked. Outside office hours, the security service also carries out checks that doors and windows are shut.

Danger alarm system

The danger alarm system to detect fires and other dangers is activated the whole time via the noris network monitoring system.

For this purpose, a silent alarm with various alarm reporting lines and a direct link to the noris network monitoring system and the linked round-the clock standby system manned by noris employees is provided. This sends a signal to the police in accordance with the emergency plan.
In the data centres, smoke detectors are connected directly to the noris network monitoring system and to the the round-the clock standby system manned by noris employees. Processing takes place in accordance with the entries in the emergency plan.
In addition, in the locations in the Deutschherrnstraße in Nürnberg, Seidlstraße and Elisabeth-Selbert-Straße in Munich and soon also in Thomas-Mann-Straße in Nürnberg, a fire alarm will be linked automatically via the fire alarm control centre to the responsible fire service. This is based on appropriate fire detectors and a fire alarm.

In the NBG3 data centre in Deutschherrnstraße, water detection bands are connected via the reporting line to the noris network monitoring system and its linked round-the clock standby system manned by noris employees. Processing takes place in accordance with the entries in the emergency plan.

Video surveillance

The data centres are subject to video surveillance both in the control channel and in the data centres themselves. As a further option, individual suites of racks and cabinets may be monitored by additional cameras. Identification for surveillance purposes, recognition and localisation of dangers as well as damage prevention and automatic alarm is carried out for the data centres by visual inspection and spot checks from the central operations room in Nürnberg.

A spot check on the digitalised movement images in the data centre can be carried out and compared with archived data (access control logs) in order to control access with regard to whether the actions carried out are legitimate.

Perimeter protection

The area covered by the offices in Deutschherrnstraße and Thomas-Mann-Straße in Nürnberg and in Elisabeth-Selbert-Straße in Munich are equipped with a cabin for the security personnel and barriers at the entrance in order to create a controlled and deterrent effect in these places. In Kilianstraße in Nürnberg, the building is to be regarded as having no contact with the general public and accordingly kept closed to the outside world. Additional measures to protect the perimeter are currently not being implemented.

Management of keys and identity passes

This is the responsibility of the human resources department that manages the relevant processes in this area, particularly the withdrawal of entitlements from employees leaving the company.

Supervision or accompaniment of third parties

The appropriate protective measures practiced by noris network are applied to access by external service providers (special process definitions on entry into the data centre: extent, time, company name, name with signature, specific access control pass, accompaniment by an employee, camera surveillance etc.), the documentation on the “ticket” ultimately rounds off the activity.

Any work to be performed by third parties is always carried out in the presence of a noris network-employee and in exceptional cases also through appropriate instructions to the employees concerned and appropriate surveillance by means of suitable measures (particularly video surveillance), evidence of entry to and departure from the data centre through the archives of the admission control system.

Access to the data centre premises during office hours

It is not foreseen that the general public will be admitted to the data centres. Only those responsible for the systems have this access. Only the IT security coordinator, the IT manager and the data centre operations manager have control over keys.
All other entitled parties require an appropriate access pass and must enter a system code. In future, a biometric function will also be implemented in the Thomas-Mann-Straße data centre in Nürnberg.

Access times are restricted to noris network AG's regular office hours.
Surveillance cameras are also viewed on a random basis during office hours from the central noris network-control room in Nürnberg.

Special procedure outside office hours

During office hours, it assumed that authorised operating personnel will normally be present in the data centre premises.

Outside these times, a dual control principle is required in order to check access to the data centre (at least contact by telephone, remote operation of the relevant door-opening system by operating staff on round-the-clock standby, backed in some cases by simultaneous viewing of the video control installation).

Should the authorised party give no sign of activity after the agreed stay in the area has ended, an employee from the operating staff investigates the area where the authorised party is supposed to be located in order to exclude any risk of personal injury. Otherwise the authorised party reports his/her departure after leaving the data centre.

The entry pass/ key providing access deposited with the security service may only be used in emergencies (particularly in the event of urgent fire-fighting operations by the fire service following automatic release of the fire alarm for the data centre in the central fire reporting system).

Control of access to the data centre

Access to the data centres with the admission passes is logged and archived by the data centre operations manager.
The fully automatic control system only admits authorised pass holders.

The video surveillance installations systematically cover all control channels and important system components. –These are evaluated by means of spot checks for any suspicious circumstances.

Inspection tours

Regular inspection tours of the data centres are carried out. These are also conducted as part of fire prevention in accordance with point 7.

Inspection tours take place daily, weekly and monthly in the data centres in accordance with a check list. The reports of the results of these tours may be inspected as hard copies held by the data centre operations manager.

Handling and security of data media

Whenever necessary, mobile data media such as tapes, discs and cassettes are stored in locked safety areas (particularly safes).

Printed records identified as strictly confidential are also stored in the safe. The safe is only accessible to an identified group of individuals who must have access to these documents.

Protected areas

Separate areas for carriers (data lines), electricity (electricity sub-distribution) and racks (racks that can be locked) and cages dedicated to individual customer projects (separate cage areas in the IT premises) have been established in the data centre to which only a defined group of individuals have access and in which secure access is possible (additional circuit in the alarm system).

Emergency exits

The data centres have emergency exits in accordance with the fire safety regulations; this ensures that an alarm is triggered if the panic function of a door, that can only be activated from the inside, is pressed.

2) Admission control

A system of user management is operated for all data processing systems requiring protection, i.e. that also covers the associated test systems.

As a matter of principle, the system of user management is operated on an individual user basis.

Password policy is based on the general requirements applicable to the creation of passwords (such as a minimum length, password complexity). If necessary, this can also be adapted to specific protection requirements by means of a policy specific to a particular system.

Moreover, as part of making a system more resilient and in consultation with the customer, restrictions on or barriers to access by visitors and/or administrators will be carried out and the blocking of user or administrator passwords after several unsuccessful attempts can be agreed as well as, if required, a password chronology and blocking of the password in the event of frequent changes and the repetition of passwords within a pre-defined period of time.

Access (and attempted access) are stored in the system log.
Sessions are subject to a defined timeout.

Clean-Desk-Policy

All employees' awareness for care in securing their working environment is refreshed in regular security awareness training sessions. Passwords must be entered free from observation, business passwords may not be used outside the company (e.g. privately at home). Confidentiality must be safeguarded. The user may not record passwords (either in writing or electronically), an exception is made for the emergency password in the safe.

Whenever necessary, additional restrictions will be placed on access to the system that the client agrees with the service provider depending on the nature of the data that is to be protected and the specific organisational data processing procedure such as for example: use of user certificates or a singe occasion password procedure instead of passwords.

3) Identity control

According to the client's requirements, noris network implements safety gateways (firewalls) and, where necessary, suitable complementary solutions such as applications firewalls, next-generation firewalls etc., that can enforce intrusion prevention or detect intrusion (e.g. after port scans etc.).

noris network will carry out virus scans for customers should this be required. The virus scanner patterns - if available - are called off from the manufacturer at regular intervals (roughly every half-hour). This process is automatically monitored. The acceptance of viruses and other threats (such as, for example, DUL) is prevented at the outset.

noris network has standard procedures and processes for security patches and reported points of weakness and also operates an automated escalation of security alarms in accordance with the German Research Network's (DFN) system of certification.

Regular security checks, such as vulnerability scans with subsequent evaluation, will be carried out if required.

4) Transfer control

Mobile data media such as tapes, discs and cassettes requiring appropriate security are stored in the safe.

All data requiring protection on mobile devices (USB sticks, DVDs) must be encoded in accordance with the latest cryptographic standards.

Old or defective devices will be destroyed by means of professional data media disposal.

Documents appropriately classified as secret or confidential are located in specially protected server or file systems, through which access by outsiders can be made difficult or prevented, in order to protect it from unauthorised disclosure or misuse. Tape libraries and disc systems are stored in appropriately protected areas (racks or cages).

Data communication

Data requiring protection is transmitted via data lines rather than physically transported in order to be able to exclude the risk of loss or data theft using these traditional methods of transportation. Encoded data transmission (e.g. via SSL, IPsec, SSL-VPN) is applied when public communications channels (such as Internet data traffic) is used.

E-mail security

A basic principle of e-mail security at noris network means: the use of encoding whenever possible (particularly TLS encoding). Employees are continually made aware of the dangers of viruses and malware. The security risks associated with e-mails are systematically reduced through virus/malware and spam filter protective measures.

5) Input control

Depending on the nature of the data to be protected, the client agrees specific organisational data processing procedures with the service provider. If necessary, noris network can provide the technical installations required for logging and archiving.

Persons entrusted with the systems covered by data protection law occupy a particular position of trust and are individually named. The activities carried out by system administration are recorded (with the time of the activity and the name of the person carrying out the activity).

As an additional measure, all employees entrusted with the management of operations are sworn to data secrecy (in accordance with § 5 BDSG) and events and advanced training courses on the subject of data security are carried out regularly.

The basis for the terms of input control constitute an effective control on access in accordance with point 2).

6) Job control

Depending on the nature of the data to be protected, the client agrees specific organisational data processing procedures with the service provider. If necessary, operations will be managed in accordance with the operating manual and all changes carried out by means of defined “change” procedures in order to ensure adequate control of the job by the client. A change process in accordance with ITIL ensures that the client gives its approval and, if necessary, enables a multi-stage change in a test and operational environment to be carried out.

As an additional measure, all employees entrusted with the management of operations are sworn to data secrecy (in accordance with § 5 BDSG) and events and advanced training courses on the subject of data security are carried out regularly.

7) Control of availability

In order to fulfil from the outset the necessity of providing a backup version, noris network AG operates its data centres in accordance with high availability standards, i.e. the risk that data is impacted by risk situations, such as water damage, lightening, breakdowns in the electricity supply or the failure of an air conditioning unit, is considerably reduced by means of specifications for a secure data centre with enhanced security requirements in accordance with BSI (German Federal Office for Information Security Technology) basic protection.

Backup

At the customer's request, noris network creates regular backups for the relevant systems as part of a defined backup procedure and a related recovery process. Backups are created in different fire protection sections in accordance with the client's requirements. Depending on the customer's requirements, the backup media are kept in the backup system at this other location or, should this be demanded by the customer, also stored as a backup medium in a safe. If necessary, the customer may specify the frequency of backups and how long they are retained in accordance with his requirements.

8) Separation rule

Depending on the customer's requirements and the adequacy of the purpose of the protection sought, noris network operates network separation in order to separate customer configurations, also within the customer configuration, in different zones (e.g. operating and test environment) that, if required, can be separated from each other by means of individual access requirements.

Annex 2: List of further processors:

Subprocessor	Activity
SpaceNet AG	Operator of data centre
Noris Networks AG	Operator of data centre
Developer, maintenance technician	simple system uses external technicians to implement new functions and maintain existing functions. The technicians do not process any personal data of the Principal, but access to Principal data cannot be excluded with certainty.