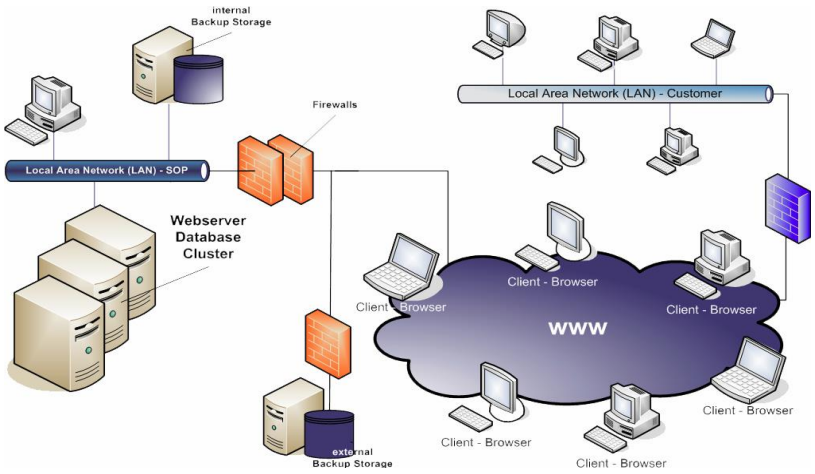
DATA SECURITY & DATA PROTECTION



DATA SECURITY

- ✓ Technical measures
- ✓ Organizational measures
- ✓ Personal measures

1. Technical measures

- redundant, server systems spatially separated from each other
  (a few buildings with a minimum 100 m of unbuilt area for the purpose of fire protection)
- redundant, back-up systems spatially separated from each other
  (a few buildings with a minimum 100 m of unbuilt area for the purpose of fire protection)
- redundant, UPS protection for emergency power supply
- redundant Internet connection
- redundant Firewalls

2. Organizational measures

Physical access control

- Both the servers and the internal back-up systems are placed in closed, air-conditioned secure rooms within locked facilities.
- All keys which enable the physical access to the server room are kept in a safe. The keys are handed out for the limited time of one entry only. SOP keeps records of all entries (date, time and names of persons passing and receiving the keys).
- The access is allowed to max. four people including the house technician, all of whom are properly trained and instructed.
- High security standards are met thanks to keeping access and attendance reports (who, when, how long), access control by the staff during the working time, and the night-time building inspections by an external private security enterprise.
- The access to the office facilities is permitted solely to SOP's employees and cleaning services under SOP's supervision.
- Other persons or guests may enter only when accompanied by an authorized person who has been entrusted with the keys.
- The SOP's management is responsible for handing out keys. The company has a register of keys with a list of people whom these have been handed over. In case an employee leaves the

company or is absent longer than a month, the keys are returned to the company management, which action is also recorded.

Storage media control

- The company uses its own VPN (Virtual Private Network) for the whole IT. Hardware and software firewalls are installed in all company's offices protecting its VPN from unauthorized access and attacks.
- All computers at the company's premises are linked with the SOP's domain. Logging in at workstations is possible only with valid access data. The access data to administrator accounts are known solely to company administrators (at present only the managing directors assume this function).
- Upon joining the company, every new employee receives a separate user identity. The rights of each user identity are restricted depending on the employee's scope of activities and the length of their employment at the company. User identities and initial passwords are provided by one of the company administrators. The access rights are deactivated in case of long absence (more than one week) or employee's leaving the company.
- All servers and sensitive server services are additionally protected with numerous user accounts, which are active for a limited period of time and whose access data are disclosed only when necessary for the purpose of completing particular tasks.
- SOP observes the following domain regulations concerning passwords: the minimal password length is 10 characters; passwords must use characters of at least 3 from 4 categories; the maximal password validity period is 30 days; the password history must include at least 12 records.
- User identity and password are exclusive to the person and cannot be transferred or disclosed.
- The remote access to the server systems is only possible via VPN (Virtual Private Network) connection and it is subordinate to the same regulations in terms of password security as the local access.
- The unauthorized access from the public network (Wide Area Network) / LAN (Local Area Network) is prevented by Fortinet Firewalls incl. AV, IPS, DoS configuration, etc.

Memory control

- All users have minimal rights necessary for discharging their duties.
- All login attempts at company computers and domain servers as well as individual sensitive services are recorded and regularly checked to secure that employees access only the sensitive data relating to the tasks they were assigned with. These administrative records are stored 12 months in the system.
- Extended rights are withdrawn after the task completion.
- All login anomalies are analysed and dealt with.
- Individual access rights within application are managed by authorized users using the role restriction settings and RWXD control.
- Individually definable Timeout-sessions help prevent the unauthorized access, should the user forget to log out from the system.

Disclosure control

- All employees are obliged not to disclose any data relating to company, customers or other involved parties and persons.

- All personal data is transferred exclusively using an encryption complying with high security standards: a secure connection with the application and with the database is guaranteed thanks to SSL (Secure Socket Layer) via public certificate „Versign Secure Site Pro“, HTTPS, OWASP, URL- and Parameter-Encryption, Captcha, etc.
- Personal data is transferred only to destinations which have a respective certification from your side. SOP keeps records of every personal data transfer. The list of currently authorized destinations for personal data transfer can be displayed in the system when needed.
- Both files containing personal data and back-up copies of databases are encrypted.
- SOP always uses the updated versions of the involved systems to guarantee the highest effectiveness of the applied encryptions.
- Every personal data query in the database is recorded in terms of its type, purpose and user.
- In principle, any transportation of data carriers with sensitive data does not take place.

Input control

- Any actions involving personal data processing such as creating new data records and changing or erasing existing ones are logged in terms of: user, introduced changes, and time (who, when, what, how, from where, where to).
- Performing the abovementioned actions is only possible with a valid password.
- Software-controlled, predefined data processing procedures, which cannot be omitted by the user, secure the traceability of data usage.

Order control

- Personal data is not disclosed or processed by any third party companies for the purpose of outsourced data processing. In other words, personal data processing takes place only within the company SOP.
- Should third-party data processing on behalf of SOP be necessary in the future, SOP shall notify the Client about it and only after receiving their written consent can the data processing be subcontracted in compliance with the highest transparency and security standards.

Availability control

- All personal data and documents are stored in one central database.
- Regular incremental back-ups and everyday complete back-ups are created for the database (please see p.5), which are stored in different locations.
- In case of data loss, the data can be restored or reset to an earlier date. Emails and other communication media which can contain personal data are stored on our servers.

Principle of purpose

- All personal data processed in SOP is voluntarily provided by the users of our services and it is used only for the purpose which is evident by its entering.
- Under no circumstances is personal data stored or processed for any other purposes.

3. Personal measures

Administrators

- System administrators are also representatives of SOP's management. There are always at least two appointed administrators: one of them assumes the function of the head administrator whereas the other one is the deputy administrator.

Training

- All SOP employees who have access to data requiring data protection are given instructions about the data processing according to data protection laws in the course of their internal training. Procedures and requirements concerning data processing are discussed in detail with every new employee.
- All employees are obliged to notify their superiors immediately, should they notice any abnormalities with regard to data protection. Provided that they are able and authorized to undertake necessary actions themselves, they are to proceed with problem solving without delay.
- All employees are obliged to non-disclosure of data relating to the company, clients, and other parties involved.

Maintenance and bug fixing

- Software updates and hardware-related maintenance works are always performed by the company's own and authorized staff.

Recognition of malfunctions

- After a flaw has been recognized, a technical record is created and sent to the designated company unit for bug fixing. The responsible unit is responsible for the prompt fault correction followed by the corresponding software rollout and patch management.

SOP
www.sop-at.com

MOBILITY-ONLINE

Data backup

✓ Transaction backups
every 15 minutes

✓ Database backups
daily / weekly / monthly / yearly

✓ Storage period

Transaction- and daily backups
30 days

Weekly backups
10 weeks

Monthly backups
18 weeks

Yearly backups
8 years

Backup media

NAS – Network Area Storage
in LAN (Local Area Network)
for transactions- and database backups
(day, week, month, year)
+
NAS – Network Area Storage
outside of LAN
= redundant backup

System/ application backups

weekly / monthly

✓ Storage period

Weekly backups
5 weeks

Monthly backups
12 months

Data destruction

When the storage period ends, the expired backups are destroyed according to the data privacy policy. The data destruction is performed according to ISO 27001 and DIN 66399 H-3.