LAP technical and organisational measures for the protection of personal data

Status January 2024

Access control: Unauthorized access must be prevented, whereby the term is to be understood spatially.

- Authorization cards, electronic access cards/ transponders, access authorization concept
- Alarm system
- Monitoring of visitors
- Limited and controlled access to security areas
- Separately secured access to the data center
- Storage of servers in locked rooms, Storage of data media under lock and key or in locked rooms
- Storage of data backups

Intrusion control: The intrusion of unauthorized persons into the data processing systems or their unauthorized use must be prevented.

- Locking of data processing equipment
- Password protection of computer workstations
- Functional and/or time-limited assignment of user authorizations
- Use of individual passwords
- Password policy with minimum password complexity requirements
- Process for assigning rights when new employees join the company
- Process for revoking rights when employees change departments
- Process for revoking rights when employees leave the company
- Commitment to confidentiality of all employees (as permitted by law)
- Controlled destruction of data media

Activity control: Unauthorized activities in Data processing systems outside of granted authorizations must be prevented.

- Authorization concept
- Regulation for restoring data from backups (who, when, on whose request)
- Regular review of authorizations
- Restriction of free and uncontrolled querying of databases
- Regular evaluation of logs (log files)
- Partial access to databases and functions (Read, Write, Execute)
- Use of security systems (software/hardware)
- Virus scanner
- Firewalls
- SPAM filters

Separation control: Data collected for different purposes must also be processed separately.

- Logical data separation (e.g. based on customer or client numbers)
- Authorization concept that takes into account the separate processing of client data from data of other clients
- Rights- and role-based access control system
- Separation of development, test and production systems

Disclosure control:

- Dispatch via VPN connection (IP-Sec)
- No disclosure without prior confidentiality agreement and only where legally permissable
- Secure deletion of data media: Physical destruction
- Paper disposal: Secure destruction of paper documents: shredder acc. to DIN 66399
- Sealed metal containers (so-called data protection garbage cans), disposal by service provider.
- Possibility of remote blocking or remote deletion of portable devices

Input control: Traceability or documentation of data management and maintenance must be ensured.

- Definition of user authorizations (profiles)
- Differentiated user permissions: Read, change, delete
- Field access for databases
- Organizational definition of input responsibilities
- Logging of entries/deletions (for defined fields)

Availability control: Data must be protected against accidental destruction or loss.

- Implementation of data protection and backup concepts
- Restricting access to server rooms to necessary personnel only
- Smoke detectors and Fire alarm systems in server rooms
- Air-conditioned server rooms
- Lightning / overvoltage protection
- Server rooms and data backups in separate fire compartment
- Accommodation of backup systems in separate premises and fire compartment
- Ensuring technical readability of backup storage media for the future
- Disaster or emergency plan (e.g. water, fire, explosion, threat of attack, crash, earthquake)
- UPS (uninterruptible power supply) solution

Resilience and resilience control: Systems must have the ability to cope with risk-related changes and have a tolerance and compensatory capability to failures.

- Hard disk mirroring
- Load balancer
- data storage on RAID systems (RAID 1 and higher)
- Identification of the various devices that make up the network and determination of their hardware version as well as their current software and firmware versions.
- External contractors and maintenance personnel are given specific access that is only active during the intervention and disabled the rest of the time.
- Identification of IT devices, assets and network systems in the organization's infrastructure.

Control procedure: A procedure for regular review, assessment and evaluation of the effectiveness of the data security measures shall be implemented.

- Continuous internal monitoring of data security measures

Order control: It must be ensured that data processed by service providers (subcontractors) on behalf of the company are only processed in accordance with the instructions of the contractor.

- Contracts with subcontractors
- If external servers are used, LAP will ensure that the server provider comply with the standard of security level as described herein.

Additional measures for remote access:

- Employees who carry out remote services are contractually obliged to confidentiality
- Remote services are only carried out in agreement with and with the consent of the customer
- Customer has the possibility to control remote services and can interrupt it at any time
- Remote services are only performed by LAP personnel
- Remote services are carried out from the respective LAP location or Germany
- Furthermore, the technical and organizational measures of the customer for the protection of its data shall apply. The customer shall ensure that access to personal data is reduced to the necessary minimum during remote access and that no access is possible to data that is not the subject of the remote services.

Additional measures for the processing of patient data

NOTE: LAP is not responsible for the availability of patient data. LAP only receives patient data for support and service purposes and will delete patient data afterwards. Availability of patient data is always the sole responsibility of the customer / client.

- LAP might get access to or receive patient data in case of support or service
- Patient data is only processed if LAP is advised to do so by customer
- If possible, LAP will only work with anonymized data
- LAP employees get training on the treatment of patient data
- Access to / Transfer of patient data to LAP only with permission of the customer
- Transfer of patient data only via a separate and secured upload facility
- LAP provides an extranet (B2B) via SharePoint for uploading patient data if necessary
- Access to extranet only with prior registration and limited access rights
- No email transfer of patient data; emails with patient data can be blocked
- Patient data is kept separately from other LAP data in a locked container environment
- Password protection for storage media of patient data
- Patient data stored on products sent to LAP for service, repair, return or exchange will be deleted by LAP
- Limited access rights to patient data (need to know / limited in time)
- Deletion of patient data as soon as data is not required anymore

Lüneburg, January 2024

L A P GMBH LASER APPLIKATIONEN
Zeppelinstr. 23
21337 Lüneburg
Deutschland

Local court of Lüneburg HRB 206423