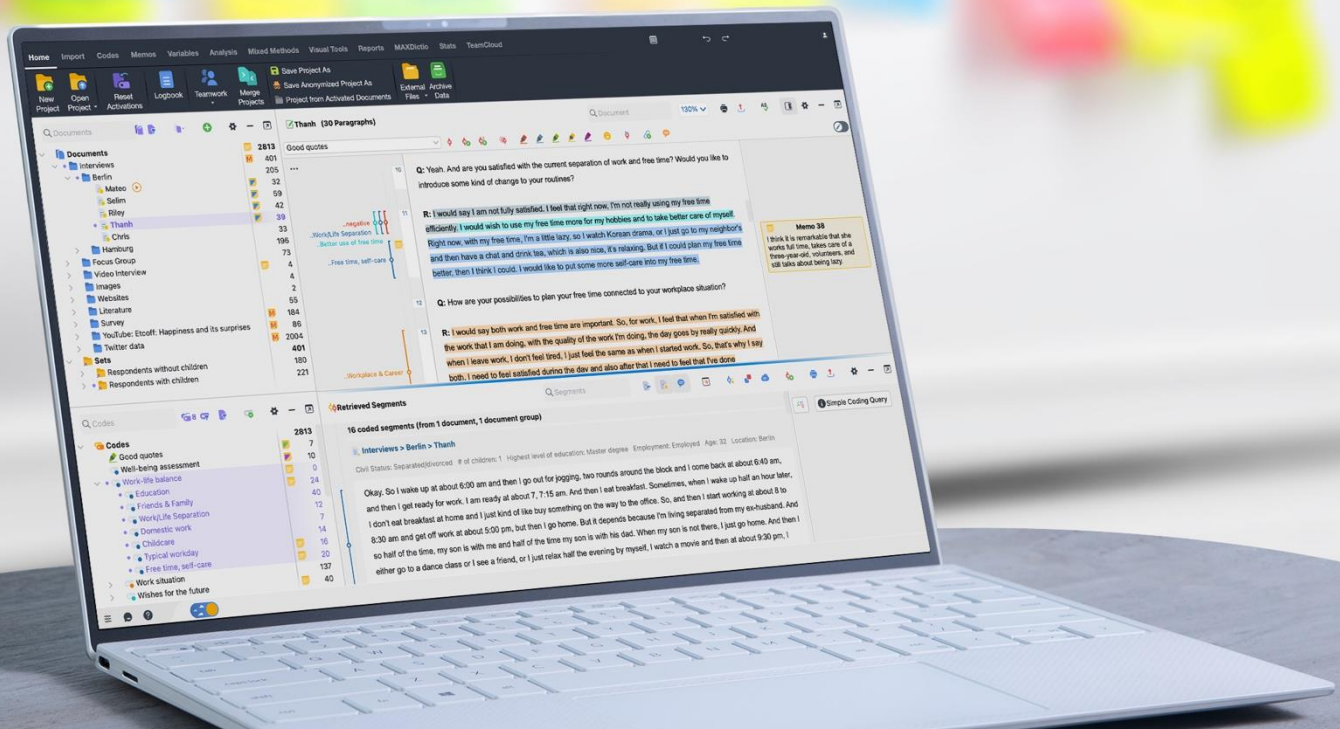
MAXQDA

Technical and organisational measures



1. confidentiality (Art. 32 para. 1 lit. b GDPR)

1.1 Access control

Measures that are suitable for preventing unauthorized persons from gaining access to data processing systems with which personal data is processed or used.

- Alarm system
- Safety locks
- Locking system with code card
- Doorbell system with camera
- Careful selection of security staff
- Careful selection of the cleaning service

1.2 Access control

Measures that are suitable for preventing data processing systems (computers) from being used by unauthorized persons.

- Login with user name and password
- Use of anti-virus software
- Use of firewall software
- Use of VPN for remote access
- Creating user profiles
- Assigning and managing user authorizations
- Assigning passwords
- Guidelines for: "Secure password" and "Delete/destroy"

1.3 Access control

Measures to ensure that persons authorized to use a data processing system can only access the data subject to their access authorization, and that personal data cannot be read, copied, changed or removed without authorization during processing, use and after storage.

- Use of document shredders
- Physical deletion of data carriers
- Proper destruction of data carriers (DIN 32757)
- Logging of access to applications, specifically when entering, changing and deleting data
- Management of rights by system administrator

- Number of administrators reduced to the "bare minimum"

1.4 Separation control

Measures to ensure that data collected for different purposes can be processed separately.

- Separation of development and test environment
- Strictly separate storage of data in different customer systems
- Providing the data records with purpose attributes/data fields
- Definition of database rights
- Control via authorization concept

1.5 Pseudonymization

The processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to appropriate technical and organizational measures.

- Internal instruction to anonymize / pseudonymize personal data as far as possible in the event of disclosure or after the statutory deletion period has expired.

2. Integrity (Art. 32 para. 1 lit. b GDPR)

2.1 Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transmission or during transport or storage on data carriers, and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

- Use of VPN
- Logging of accesses and retrievals
- Personal data that is passed on on behalf of customers is only passed on to the extent that this has been agreed with the customer or is necessary for the provision of the contractual service for the customer.

- Employees of VERBI GmbH who work in customer support are instructed with regard to the permissible use of data and the modalities of passing on data.

2.2 Entry control

Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, modified or removed from data processing systems.

- Technical logging of the entry, modification and deletion of data
- Overview of which programs can be used to enter, change or delete which data Forwarding
- Traceability of data entry, modification and deletion through individual user names (not user groups)
- Clear responsibilities for deletions and reminder system for deletion.

3. Availability and resilience (Art. 32 para. 1 lit. b GDPR)

Measures to ensure that personal data is protected against accidental destruction or loss.

- Fire and smoke detection system
- Server room temperature and humidity monitoring
- Air-conditioned server room
- Protective socket strips Server room
- Fire extinguisher Server room
- Uninterruptible power supply (UPS)
- Logging of accesses and retrievals
- Implementation of the backup & recovery concept
- Regular data recovery tests and logging of the results
- Storage of backup media in a secure location outside the server room
- No sanitary connections in or above the server room.

4. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. d GDPR; Art. 25 para. 1 GDPR)

4.1 Data protection measures

- Central documentation of all procedures and regulations on data protection with access for employees as required/authorization on the intranet
- Regular review of the effectiveness of technical protection measures

- Engagement of an External Data Protection Officer (kontakt@datenschutzrechte.de)
- A DST (Data Protection and Information Security Team) has been set up to plan, implement, evaluate and adjust measures in the area of data protection and data security
- The data protection impact assessment is carried out as required
- VERBI GmbH complies with the information obligations under Art. 13 and 14 GDPR
- Formalized process for processing requests for information from data subjects is in place

4.2 Incident-Response-Management

Support in responding to security breaches

- Use of firewall and regular updates
- Use of spam filters and regular updates
- Use of virus scanners and regular updates
- Support from IT crisis experts and data protection lawyers as part of cyber risk insurance
- Documentation of security incidents and data breaches, e.g. via ticket system
- All employees are instructed and trained to ensure that data protection incidents are recognized and reported to the DPO immediately.
  The training courses are held regularly to ensure that the content is continuously updated.

4.3 Data protection friendly default settings

Privacy by design / Privacy by default

- The principle of necessity and data minimization is taken into account.
- No more personal data is collected than is necessary for the respective purpose.

4.4 Order control (outsourcing to third parties)

Measures to ensure that personal data processed on behalf of the client can only be processed in accordance with the client's instructions.

- Selection of the contractor under due diligence aspects (in particular with regard to information security).
- Regular monitoring of contractors.
- The principle of necessity and data minimization is taken into account
- Conclusion of the necessary agreement on order processing or EU standard contractual clauses.
- A regularly updated list of third-party service providers and subprocessors can be found on our website.