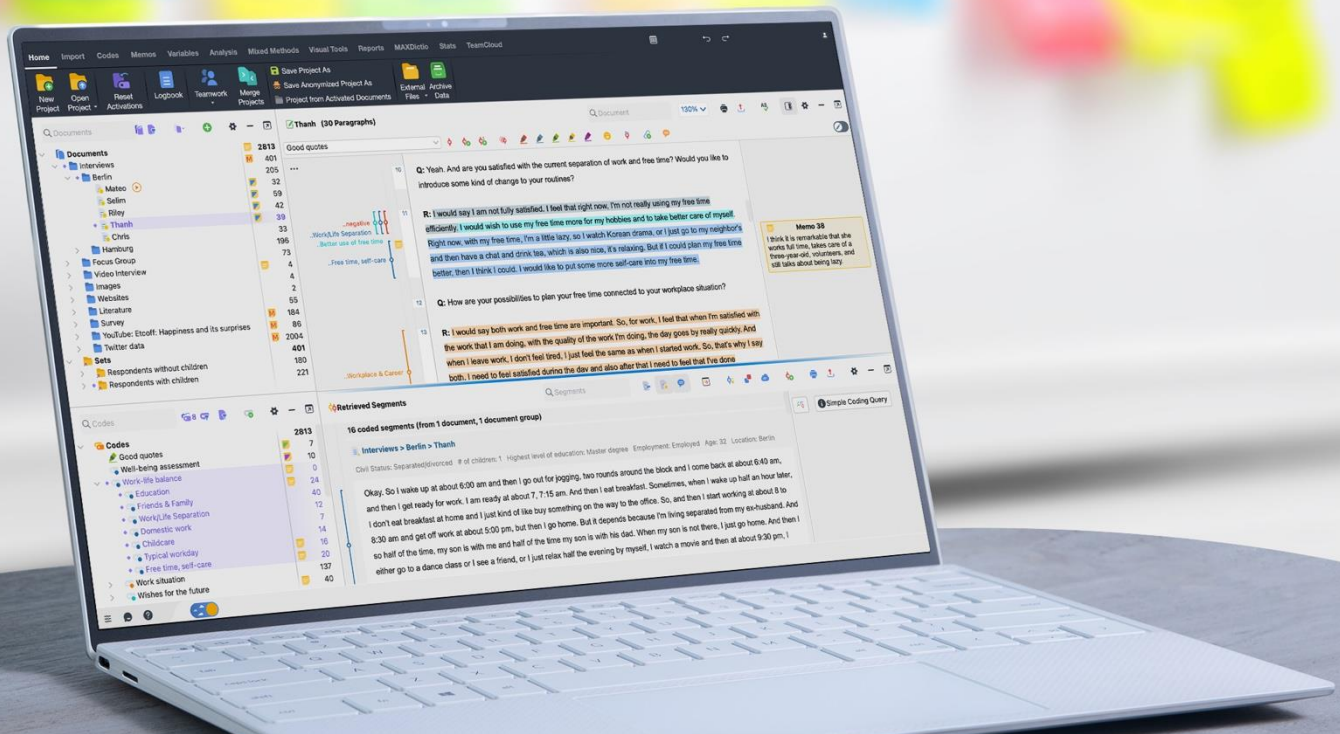
MAXQDA

Technische und organisatorische Maßnahmen



1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- Alarmanlage
- Sicherheitsschlösser
- Schließsystem mit Codekarte
- Klingelanlage mit Kamera
- Besucherbuch
- Sorgfalt bei Auswahl des Wachpersonal
- Sorgfalt bei Auswahl des Reinigungsdiensts

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

- Login mit Benutzername und Passwort
- Einsatz von Anti-Viren Software
- Einsatz einer Firewall Software
- Einsatz von VPN bei Remote-Zugriffen
- Erstellen von Benutzerprofilen
- Zuordnung und Verwaltung von Benutzerberechtigungen
- Passwortvergabe
- Richtlinien für: „Sicheres Passwort“ und „Löschen/Vernichten“

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass

personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Einsatz von Aktenvernichtern
- Physische Löschung von Datenträgern

- Ordnungsgemäße Vernichtung von Datenträgern (DIN 32757)
- Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Trennung von Entwicklungs- und Testumgebung
- Streng getrennte Speicherung der Daten in unterschiedlichen Kundensystemen
- Versehen der Datensätze mit Zweckattributen/Datenfeldern
- Festlegung von Datenbankrechten
- Steuerung über Berechtigungskonzept

1.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren.

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Einsatz von VPN
- Protokollierung der Zugriffe und Abrufe
- Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden erfolgen, erfolgen nur in dem Umfang, wie es mit Kunden abgesprochen ist oder soweit es zur Erbringung der vertraglichen Leistung für den Kunden erforderlich ist.
- Mitarbeiter der VERBI GmbH, die im Kundensupport tätig sind, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

2.2 Eingangskontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können Weitergabe
- Nachvollziehbarkeit von Eingabe Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Klare Zuständigkeiten für Löschungen und Erinnerungssystem zur Löschung.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Feuer- und Rauchmeldeanlage
- Serverraumüberwachung Temperatur und Feuchtigkeit
- Serverraum klimatisiert
- Schutzsteckdosenleisten Serverraum
- Feuerlöscher Serverraum
- Unterbrechungsfreie Stromversorgung (USV)
- Protokollierung der Zugriffe und Abrufe
- Durchführung des Backup- & Recoverykonzepts
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse

- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

4.1 Datenschutz-Maßnahmen

- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung im Intranet
- Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird regelmäßig durchgeführt
- Bestellung eines externen Datenschutzbeauftragten (kontakt@datenschutzrechte.de)
- Es ist ein (DST Datenschutz- und Informationssicherheits-Team) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt
- Die Datenschutz-Folgenabschätzung wird bei Bedarf durchgeführt
- Die VERBI GmbH kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
- Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden.

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Spamfilter und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Unterstützung durch IT-Krisenexpert:innen und Datenschutzanwält:innen im Rahmen einer Cyber Risk Versicherung
- Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
- Alle Mitarbeitende sind dahingehend instruiert und geschult, dass Datenschutzvorfälle erkannt und unverzüglich dem DSB gemeldet werden. Die Schulungen werden regelmäßig durchgeführt, um eine kontinuierliche Aktualisierung der Inhalte zu gewährleisten.

4.3 Datenschutzfreundliche Voreinstellungen

Privacy by design / Privacy by default

- Dem Grundsatz der Erforderlichkeit und Datenminimierung Rechnung wird getragen.
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

4.4 Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insb. hinsichtlich Informationssicherheit).
- Regelmäßige Kontrolle der Auftragnehmer.
- Dem Grundsatz der Erforderlichkeit und Datenminimierung Rechnung getragen wird.
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln.
- Eine regelmäßig aktualisierte Liste der Drittdienstleister- und Unterauftragsverarbeiter finden Sie auf unserer Webseite.