TOM QuaMath (auf SDM-Basis)

Das Medieninstitut
der Länder

Inhaltsverzeichnis

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO der Infrastruktur von **«QuaMath»**

beim

FWU Institut für Film und Bild in Wissenschaft und Unterricht gGmbH

vertreten durch die Geschäftsführer Andreas Koschinsky, Rüdiger Nill

HR: AG München B 2636

Bavariafilmplatz 3

82031 Grünwald

Stand: 27.05.2024 Version 1.0

1. Präambel

Dieses Dokument ist nur gültig als Anlage eines Auftragsverarbeitungsvertrags.
Die in diesem Dokument definierten technischen und organisatorischen Maßnahmen (TOM) sind eine Ergänzung zu den im Auftragsverarbeitungsvertrag vereinbarten Regelungen zur Ausgestaltung der in Artikel 32 definierten Anforderungen der DSGVO. Für die Verarbeitung im Auftrag gelten die Vorgaben des Auftragsverarbeitungsvertrags vollumfänglich.
QuaMath bedient sich zu Erbringung der Dienstleistung Unterauftragsverarbeiter (im folgenden „Dienstleister"). Die technischen und organisatorischen Maßnahmen der Dienstleister sind in einem eigenen Dokument erläutert. Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.
QuaMath erfüllt diesen Anspruch durch folgende Maßnahmen:

2. Maßnahmen der Datensicherheit

2.1. Maßnahmen zur Gewährleistung der Vertraulichkeit und Integrität der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO)

2.1.1. Maßnahmen zur Gewährleistung von Vertraulichkeit

Das Schutzziel der Vertraulichkeit stellt sicher, dass personenbezogene Daten nur von Personen eingesehen, verändert oder gar gelöscht werden können, die dazu berechtigt sind. QuaMath sorgt dafür, dass nur Befugte die Möglichkeit haben, entsprechende Daten abzurufen.

Durch Verschlüsselung der übertragenen Daten wird ein hohes Niveau an Vertraulichkeit geschaffen.

Darüber hinaus stellt QuaMath auch durch entsprechende Maßnahmen (u.a. Signierung) zum Schutz der Integrität sicher, dass diese Daten unverfälscht übertragen werden.

Bei dem Einsatz des Personals und externer Dienstleister wird die fachliche Eignung und Freiheit von Interessenkonflikten mittels eines definierten Prozesses überprüft.

Zutrittskontrolle

In den Gebäuden wird der Zugang zu kritischer Infrastruktur durch Pforte und Videoüberwachung überwacht und aufgezeichnet. Die Mitarbeiter sind geschult, betriebsfremde Personen zu begleiten. QuaMath bedient sich zu Erbringung der Dienstleistung der Verarbeitungsanlagen (Server u.ä.) von Dienstleistern. QuaMath besitzt keine eigenen Verarbeitungsanlagen.

Zugangskontrolle

Zwei-Faktor-Authentifizierung

Der Einsatz von Hard- und Software bei QuaMath durch Mitarbeiter wird zentral administriert und unterliegt festgelegten Richtlinien. Administrative Zugänge sind durch 2-Faktor Authentifizierung geschützt. Es bestehen Benutzerprofile mit unterschiedlichen Berechtigungen. Um Zugang zu den IT-Systemen zu erhalten, müssen die Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen auf Antrag des jeweiligen Vorgesetzten von Administratoren vergeben. Vom Nutzer vergebene Passwörter werden grundsätzlich den Administratoren nicht angezeigt, können jedoch neu vergeben werden (nach dem Speichern wird das Passwort ebenfalls nicht mehr angezeigt)

Sichere Passwörter

Es bestehen Passwortrichtlinien. Die Beschäftigten sind zur Passwortnutzung verpflichtet. Der Benutzer erhält bei erstmaligen Anmeldungen einen Benutzernamen und ein Initialpasswort, das bei erster Anmeldung geändert werden muss. Die Passwortvorgaben beinhalten eine Mindestpasswortlänge von 8 Zeichen, wobei das Passwort aus Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen bestehen muss. Die Passwörter werden üblicherweise alle 180 Tage gewechselt. Passworthistorien sind hinterlegt. Zuletzt verwendete Passwörter können deshalb nicht noch einmal verwendet werden. Passwörter werden grundsätzlich verschlüsselt gespeichert. Externe Passwörter müssen im FWU-Passwort-Manager gespeichert werden. Der FWU-Passwort-Manager enthält einen eigenen Benutzerbereich und einen Teamspeicher. Die Authentifikation am FWU-Passwort-Manager erfolgt durch Benutzername und Passwort. Fehlerhafte Anmeldeversuche werden protokolliert.

Alle Beschäftigten sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese bzw. ihr Büro verlassen. Es tritt eine automatische Bildschirmsperre nach wenigen Minuten ein, wenn ein Mitarbeitercomputer nicht genutzt wird.

Zugriffskontrolle

Es sind Maßnahmen verwirklicht, die gewährleisten, dass die Nutzungsberechtigten eines Datenverarbeitungssystems 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. Dazu besteht ein umfassendes Nutzer-Berechtigungskonzept. Es gibt ein rollen- und gruppenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten. Die Verwaltung der Nutzerrechte erfolgt durch die Systemadministratoren . Insgesamt ist ein System von Befugnissen abgestufter Zugriffsberechtigungen errichtet.

Die Zugriffe auf Anwendungen werden protokolliert.

Datenträger und Aktenordner werden in abschließbaren Schränken aufbewahrt. Es werden speziell ausgewählte Dienstleister zur Aktenvernichtung (inkl. Protokollierung der Vernichtung) herangezogen, die eine Vernichtung nach DIN 66399 gewährleisten.

Den Beschäftigten ist es untersagt, nicht genehmigte Software auf den IT-Systemen zu installieren. Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

Trennung

Es sind Maßnahmen verwirklicht, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Logische Trennung von Anwendungen.
- Logische Trennung bei der Datenhaltung.
- Logische Trennung bei der Speicherung von personenbezogenen Daten verschiedener Verantwortlicher, ausgenommen solche personenbezogenen Daten, die zur Auftragsabwicklung erforderlich sind, wie Name, E-Mail, Telefonnummer der Ansprechpartner.
- Trennung von Test-, Entwicklungs- und Produktivsystemen.

2.1.2. Maßnahmen zur Sicherstellung der Integrität

Der Grundsatz der „Integrität" (Art. 5 Abs. 1 lit. f) DSGVO) sieht vor, dass personenbezogene Daten in einer Art und Weise verarbeitet werden müssen, die den Schutz vor „unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen" gewährleistet.

Bei QuaMath wird die Integrität der verarbeiteten Daten durch unterschiedliche Maßnahmen sichergestellt.

Die folgenden Maßnahmen dienen der Gewährleistung der Integrität und zur Feststellung von Integritätsverletzungen. Damit werden insbesondere die Integrität, Richtigkeit und angemessene Überwachung der Verarbeitung erreicht.

Eingabekontrolle

Es sind Maßnahmen verwirklicht, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dazu wird die Eingabe, Änderung und Löschung von Daten auf Datenbankebene protokolliert. Für die Nutzer gibt es entsprechend individuelle Benutzernamen. Durch das Berechtigungskonzept wird die Nachvollziehbarkeit zusätzlich unterstützt. Papierunterlagen, von denen Daten in ein Datenverarbeitungssystem übernommen wurden, werden in Akten sicher aufbewahrt.

Weitergabekontrolle

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

Für den Fernzugriff im sogenannten Home Office auf die internen Systeme durch Mitarbeitende des FWU werden Sicherungsmethoden nach dem aktuellen Stand der Technik genutzt (VPN-Tunnel).

Signierung von Nachrichten und Transportverschlüsselung

Der Datentransfer von und zu externen Systemen wird mit kryptographischen Mechanismen umgesetzt:

- Signierung der Nachrichten (abhängig des jeweils verwendeten Protokolls des Identity-Providers, siehe unten).
- Transportverschlüsselung per HTTPS mit einem SSL-Zertifikat mit 2048 Bit Verschlüsselung und kurzlaufende Zertifikatsdauer (jeweils 1 Jahr). Durch jährlichen Tausch des SSL-Zertifikats wird zusätzlich die Angriffsmöglichkeit erschwert und das Sicherheitsniveau erhöht.
- Sicherung von (kurzzeitig) abgespeicherten Daten ("Data-At-Rest") durch Verschlüsselung.

Die Validierung und das Sicherstellen der Korrektheit der Nutzerdaten wird durch QuaMath sichergestellt.

QuaMath stellt die Integrität und Richtigkeit der Daten unterschiedlich sicher, indem es technisch unterbindet bzw. sehr erschwert, diese Daten zu manipulieren (z. B. durch Man-in-the-Middle-Attack).

Die Beschäftigten werden regelmäßig zu Datenschutzthemen geschult. Sie wurden auf einen vertraulichen Umgang mit personenbezogenen Daten verpflichtet.

Behebung und Abmilderung von Datenschutzverletzungen

Das Ziel der Abmilderung von Datenschutzverletzungen wird neben der Verwendung von Signaturen und Verschlüsselung durch die nachfolgende weitere Maßnahme sichergestellt:

- Maßnahmen zur Erreichung der Speicherbegrenzung

Weiterhin werden folgende Vorkehrungen zur Abmilderung von Datenschutzverletzungen getroffen:

- Monitoring und Benachrichtigung von Auffälligkeiten in Logdateien
- Integriertes Scannen nach Malware oder verdächtigem Code innerhalb der Buildpipeline
- Regelmäßige Durchführung von externen Sicherheitsaudits
- Regelmäßige Updates von Software Libraries
- Kontinuierliches Schwachstellenmanagement („Vulnerability Management“) durch den Einsatz von internen Vulnerability Scannern und Nutzung von „Security Intelligence“-Feeds

Datenschutzverletzungen werden, sobald bekannt, anhand von Logdaten ausgewertet und durch geeignete Maßnahmen (z. B. Behebung von Sicherheitsschwachstellen oder Fehlkonfigurationen) behoben.

Bei der Verwendung von Open-Source oder Third-Party Software Komponenten, werden nur tatsächlich verwendete Funktionen aktiviert und weitere Code Bestandteile soweit möglich und erforderlich deaktiviert.

Veränderungskontrolle

Es sind Maßnahmen verwirklicht, die (berechtigte oder unberechtigte) Veränderungen gespeicherter oder übertragener Daten nachträglich feststellbar machen

Identifizierung und Authentifizierung

Bereitgestellte Identitäten der Heimatorganisationen werden durch den jeweiligen Betreiber des ID-Management im Vorfeld identifiziert und legitimiert.

Nutzerdaten sind über die Userinfo-Schnittstelle von QuaMath nur durch die jeweiligen Nutzer abrufbar. Das Abrufen von Nutzerinformationen anderer Nutzer ist nicht möglich, da nur der Zugriff anhand eines individuellen Access Tokens möglich ist.

2.2. Maßnahmen zur Datenminimierung und Speicherbegrenzung

2.2.1. Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)

Der Grundsatz der „Datenminimierung" aus Art. 5 Abs. 1 lit. c) DSGVO, bzw. der „Datensparsamkeit" aus § 71 BDSG, steht in engem Zusammenhang mit dem Grundsatz der Zweckbindung und fordert, dass die Datenverarbeitung auf das für den verfolgten Zweck notwendige Maß zu beschränken ist.

Im Rahmen von QuaMath werden Daten nur in dem Umfang und für die Dauer erhoben, wie sie zur Erreichung des jeweiligen Zwecks erforderlich sind.

2.2.2. Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO)

Personenbezogene Daten dürfen nach dem Grundsatz der „Speicherbegrenzung" (Art. 5 Abs. 1 lit. e) DSGVO) nur so lange in einer Form, die die Identifizierung der betroffenen Personen ermöglicht, gespeichert werden, wie es für die Verarbeitungszwecke erforderlich ist.

2.3. Maßnahmen zur Pseudonymisierung und Aggregierung

Bei Nutzungsübersichten und Auswertungen werden Daten aggregiert (zusammengefasst), um Rückschlüsse auf einzelne Personen zu vermeiden

2.4. Maßnahmen zur Verschlüsselung personenbezogener Daten

Der Datentransfer von und zu externen Systemen wird mit kryptographischen Mechanismen umgesetzt:

- Signierung der Nachrichten (abhängig des jeweils verwendeten Protokolls des Identity-Providers, siehe unten)
- Transportverschlüsselung per HTTPS mit einem SSL-Zertifikat mit 2048 Bit Verschlüsselung und kurzlaufende Zertifikatsdauer (jeweils 1 Jahr). Durch jährlichen Tausch des SSL-Zertifikats wird zusätzlich die Angriffsmöglichkeit erschwert und das Sicherheitsniveau erhöht.
- Sicherung von (kurzzeitig) abgespeicherten Daten ("Data-At-Rest") durch Verschlüsselung.

2.5. Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b DSGVO)

2.5.1. Verfügbarkeit

Die „Verfügbarkeit" wird in Art. 32 Abs. 1 DSGVO gefordert, wobei die Verfügbarkeit für Systeme und Dienste in Art. 32 Abs. 1 lit. b) DSGVO und die Verfügbarkeit von Daten in Art. 32 Abs. 1 lit. c) DSGVO gefordert ist.

Es werden Maßnahmen angewendet,, die gewährleisten, dass die eingesetzten Datenverarbeitungssysteme jederzeit verfügbar sind und einwandfrei funktionieren (Lauffähigkeit) und personenbezogene Daten gegen

zufällige Zerstörung oder Verlust geschützt sind. Dazu gehören eine unterbrechungsfreie Stromversorgung (USV) sowie IT-Infrastruktur-Komponenten (Alarmanlage und Klimaanlagen in den IT-Räumen). Temperatur und Feuchtigkeit werden überwacht. Der Serverraum ist nicht unterhalb von sanitären Anlagen gelegen und es gibt keine Wasserleitungen im bzw. über den Server-Rechnern.

Generell gibt es Schutzsteckdosenleisten für EDV-Geräte. Ebenfalls gibt es Feuer- bzw. Rauchmeldeanlagen und Feuerlöschgeräte an mehreren, entsprechend gekennzeichneten Stellen im Gebäude.

Ein Ausfall der IT am FWU führt zu keinem Ausfall von QuaMath.

Die TOM zur Vertraulichkeit dienen auch der physischen Sicherung und sind damit zugleich Maßnahmen zur Gewährleistung der Verfügbarkeit der Systeme.

Es bestehen Vertretungsregelungen für abwesende Mitarbeiter.

Schutz vor äußeren Einflüssen
Der Schutz vor äußeren Einflüssen (Schadsoftware/Malware, Sabotage z.B. DDOS, höhere Gewalt) ist sichergestellt (Belastbarkeit der Systeme).

Die **Verfügbarkeit** des Gesamtsystems wird durch folgende Maßnahmen erreicht:

- Containerisierung der Anwendungen, Komponenten und Dienste
- Monitoring und pro-aktives Skalierung anhand der Auslastung
- Fail-Over Lösungen, bei denen weitere Instanzen gestartet werden sowie weitere Skalierung über weitere RZ-Cluster
- Deployment in beliebigen anderen Cloud-Umgebungen möglich
- Regelmäßige Durchführung von Last-Tests sowie Beachtung der Ressourcen Nutzung und Auslastung bereits während der Entwicklung durch Profiling der Anwendungen
- keine Abhängigkeit von Hardware oder physikalischer Infrastruktur, komplette Virtualisierung
- Dokumentation der entwickelten Lösungen durch Dienstleister
- interne Dokumentation zur Administration des Systems
- Dokumentation eines Notfallkonzepts
- Vertretungsregelungen für abwesende Mitarbeitende sowie Nutzung von Verteilern für Team-Kommunikation

Das **Wiederherstellbarkeit** des Gesamtsystems wird durch die nachfolgend beschriebenen Maßnahmen sichergestellt.

- Automatisiertes Deployment ohne Abhängigkeit von spezifischer Hardware
- Verwendung von offenen Schnittstellen um Hersteller- und systemunabhängig QuaMath zu betreiben, wechseln oder wiederherstellen zu können

Das System kann jederzeit wiederhergestellt werden.

Zusätzlich werden die Konfigurationsdaten des System benötigt. Diese werden in einer relationalen Datenbank persistiert und werden regelmäßig gesichert. Die Wiederherstellung der Datenbank dauert nur wenige

Sekunden und beträgt derzeit nur wenige Megabyte an Speicher. Das Datenbankmanagement und die Datensicherung wird über die Infrastruktur von der Firma Netzhaut GmbH gesichert.

Anfertigung von Sicherheitskopien
Sicherheitskopien werden nach folgenden Vorgaben erstellt:

Externes Backup (selbst durchgeführte Sicherungen):

- Backup-Server bei Servern der Netzhaut GmbH in Würzburg.
- 1 x täglich
- kann per Script wiederhergestellt werden
- die jeweils letzten drei Backups plus ältere von ausgewählten Zeiträumen (z. B. jeweils eines der letzten vier Wochen)

2.6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der vorgenannten Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

Es erfolgen regelmäßige Prüfungen des Datenschutzbeauftragten und der IT-Abteilung auf Einhaltung der festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme. Ebenfalls wird turnusmäßig überprüft, ob die festgelegten TOM ihren Zweck unverändert erfüllen und auf dem aktuellen Stand der Technik sind.

Informationen über neu auftretende Schwachstellen und andere Risikofaktoren werden unverzüglich verarbeitet und ggf. an die Beschäftigten weitergegeben.

Es erfolgen Evaluierungen durch Betroffene und Nutzer.

2.6.1. Auftragskontrolle

Insofern Qua Math als Auftragsverarbeiter tätig wird, unterrichtet er den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt. Er unterstützt den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Es werden intern Maßnahmen getroffen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können. Sofern der QuaMath als Auftragnehmer Dienstleister im Sinne einer Unterauftragsverarbeitung einsetzt, werden die folgenden organisatorische Maßnahmen mit diesen geregelt:

- vorherige Prüfung der vom Unterauftragsverarbeiter getroffenen Sicherheitsmaßnahmen und deren
- Dokumentation im Rahmen einer Zuverlässigkeitsprüfung
- Auswahl des Unterauftragsverarbeiter unter Sorgfaltsgesichtspunkten (in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Unterauftragsverarbeitung
- schriftliche Weisungen an den Unterauftragsverarbeiter
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Unterauftragsverarbeiter

- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung bzw. Rückgabe von Daten nach Beendigung des Unterauftragsverarbeitung
- Auditierung des Unterauftragsverarbeiters im Bedarfsfall

3. Auf den Schutz Betroffener ausgerichtete Maßnahmen

3.1. Maßnahmen zur Gewährleistung der Zweckbindung personenbezogener Daten (Nichtverkettung)(Art. 25 Abs. 2 DSGVO, Art. 32 Abs. 1 lit. a), d) DSGVO)

Daten, die für einen bestimmten Zweck erhoben worden sind, dürfen nicht für andere Zwecke verarbeitet werden, (Art. 5 Abs. 1 lit. b DSGVO).

Es wird die Verkettung durch die implementierte Datenminimierung erschwert.

3.1.1. Maßnahmen zur Gewährleistung der Nichtverkettung

Durch Zweckbindung der Verarbeitungs-, Nutzungs- und Übermittlungsrechte wird die Möglichkeit zur Verkettung von Daten reduziert.

Durch ein entsprechendes Rollen- und Rechtekonzept mit abgestuften Zugriffsrechten durch die verantwortliche Stelle, sichere Authentifizierungsverfahren wird die Nichtverkettung zusätzlich unterstützt.

Auch durch entsprechende Qualitätssicherung der entwickelten Software wird das Gewährleistungsziel der Nichtverkettung unterstützt und regelmäßig kontrolliert.

Der Grundsatz der „Zweckbindung" aus Art. 5 Abs. 1 lit. b) DSGVO beschreibt die Verpflichtung, Daten nur für den Zweck zu verarbeiten, zu dem sie erhoben wurden. Eine darauffolgende Verarbeitung für weitere Zwecke muss laut Art. 6 Abs. 4 DSGVO mit dem ursprünglichen Zweck kompatibel sein und die Umstände der Verarbeitung berücksichtigen. Sofern dies nicht klar gegeben ist, wären die betroffenen Personen über ihr Widerspruchsrecht zu informieren.

3.2. Maßnahmen zur Gewährleistung der Transparenz für Betroffene, Verantwortliche und Kontrollinstanzen

Es sind folgende Maßnahmen verwirklicht:

- Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren
- Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren
- Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen
- Dokumentation von Widersprüchen

- Protokollierung von Zugriffen und Änderungen
- Nachweis der Quellen von Daten (Authentizität)
- Versionierung
- Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts
- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept

3.2.1. Maßnahmen zur Sicherstellung von Transparenz

Die „Transparenz" zählt zu den tragenden Grundsätzen der Verarbeitung personenbezogener Daten, der in zahlreichen Regelungen der DSGVO zu finden, und in Art. 5 Abs. 1 lit. a) DSGVO festgeschrieben ist..

Zur Gewährleistung der Transparenz werden alle Verarbeitungstätigkeiten dokumentiert und mit externen Dienstleistern (z. B. Webhosting, Cloud-Orchestrierungs, Software-Entwicklung) regelmäßig geprüft und aktualisiert.

Durch entsprechende Software Architektur und Design wird sichergestellt, dass alle Änderungen protokolliert und nachvollziehbar dokumentiert werden (z. B. Historie, Timestamps bei Änderungen, Änderung durch Nutzer, Art der Änderung, Versionierung).

Rechenschafts- und Nachweisfähigkeit

Durch die „Rechenschaftspflicht" (Art. 5 Abs. 2 DSGVO) werden die Verantwortlichen verpflichtet, den Nachweis zu erbringen, dass die in Art. 5 Abs. 1 DSGVO formulierten Grundsätze zur Verarbeitung personenbezogener Daten eingehalten werden. Nach Art. 24 Abs. 1 S. 1 DSGVO steht der Verantwortliche in der Pflicht, sicherzustellen und den Nachweis zu erbringen, dass die Verarbeitung gemäß der DSGVO erfolgt.

Die Rechenschafts- und Nachweisfähigkeit wird durch ein Datenschutzkonzept einschließlich der Anlagen und geeignete Protokolle erfüllt.

Einwilligungsmanagement

Es ist ein Einwilligungsmanagement notwendig, da die Rechtsgrundlagen zur Verarbeitung von personenbezogenen Daten auf Art. 6 Abs. 1 lit. a) beruhen.

3.3. Maßnahmen zur Gewährleistung der Betroffenenrechte (Intervenierbarkeit)

Intervenierbarkeit als Konzept zur Umsetzung informationeller Selbstbestimmung nicht durch eine "Opt-Out" Möglichkeit für Nutzer angeboten, da wir es hier mit Daten im schulischen Kontext zu tun haben. In diesem Fall, wird die gesetzliche Grundlage hierfür über die Schulgesetzgebung der einzelnen Bundesländer geschaffen.

3.3.1. Löschbarkeit von Daten

Benutzerdaten werden zweckgebunden gespeichert und nach Entfallen der Voraussetzung gelöscht.

3.3.2. Unterstützung bei der Wahrnehmung von Betroffenenrechten

QuaMath als Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt. Er befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

Für den Fall, dass QuaMath selbst betroffen ist, steht eine Supportmöglichkeit in Form eines Kontaktformulars und einer Telefonnummer bereit, die der Annahme der Anfrage dient und deren Eingang bestätigt. Nach

Identifizierung/Legitimierung der betroffenen Person werden die verarbeiteten Daten über die betroffene Person zusammengestellt und um Daten Dritter bereinigt. Diese Auskunft wird dem Antragenden übermittelt.

3.3.3. Berichtigungsmöglichkeit von Daten

Betroffene haben das Recht auf Berichtigung aus Art. 16 DSGVO. QuaMath stellt hierfür Kontaktmöglichkeit bereit.

3.3.4. Einschränkbarkeit der Verarbeitung von Daten

Es besteht das Recht der Betroffenen auf Einschränkung der Verarbeitung (Art. 18 DSGVO). Auf Antrag der betroffenen Person werden die gespeicherten personenbezogenen Daten markiert mit dem Ziel, ihre künftige Verarbeitung einzuschränken, sofern dies zulässig ist, und insofern diese Daten durch QuaMath verarbeitet und gespeichert werden. Auf die Tatsache, dass die Verarbeitung der personenbezogenen Daten beschränkt wurde, wird im System unmissverständlich hingewiesen. Die technischen und organisatorischen Einschränkungen der Verarbeitung werden auch bei ggf. vorhandenen Sicherungskopien der Daten angewendet.

Die Verarbeitung der Nutzerdaten wird auf verschiedenen Ebenen ermöglicht.