Vereinbarung zur Auftragsverarbeitung (AVV)

nach EU-Datenschutz-Grundverordnung
(Elektronischer Abschluss)

English translation below.

Zwischen dem

Nutzer der Software QVANTUM als Software as a Service

- Auftraggeber -

und dem

Anbieter der Software QVANTUM als Software as a Service
(Thinking Networks AG, Markt 45-47, D-52062 Aachen)

- Auftragnehmer -

über Auftragsverarbeitung i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung (DS-GVO).

Präambel

Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der im Hauptvertrag zur Leistungserbringung in ihren Einzelheiten beschriebenen Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag zur Leistungserbringung in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Aus dem Hauptvertrag zur Leistungserbringung ergeben sich Gegenstand und Dauer des Auftrags sowie Art und Zweck der Verarbeitung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

(1) Art der Daten:

a. Personenstammdaten (z.B. Name, Adresse, Telefonnummer, E-Mail)
b. Vertragsstammdaten (Vertragsbeziehungen)
c. Kundenhistorie
d. Planungs- und Steuerungsdaten

(2) Art und Zweck der Datenverarbeitung

a. Erhaltung der Gebrauchstauglichkeit,
b. Anpassung neuer Versionen an eine veränderte Programmumgebung,
c. Mängelbeseitigung,

d. Hotline,
e. Fernwartung,
f. Unterstützung des Auftraggebers bei Tests durch die erforderlichen Testszenarien
g. Bereitstellung von IT-Infrastruktur, sowie Speicherung und Sicherung der Daten im Rahmen der Cloud-Hosting-Dienste des Auftragnehmers,
h. Diagnose und Wartung per Fernzugriff, bei denen eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann,
i. Zusatzunterstützungsleistungen gegen gesonderte Vereinbarung und Vergütung

(3) Kategorien betroffener Personen

Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrages Betroffenen umfasst:

a. Kunden
b. Beschäftigte

Nicht Gegenstand dieser Auftragsverarbeitung sind personenbezogene Daten des Auftraggebers, die der Auftragnehmer zu eigenen Geschäftszwecken verarbeitet.

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Hauptvertrages zur Leistungserbringung, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

§ 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Hauptvertrag zur Leistungserbringung und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich. Der Auftraggeber ist „Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DS-GVO. Die Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Gleiches gilt für die Auftragsverarbeitung durch Subunternehmer gem. § 7 dieser Vereinbarung.

(2) Die Weisungen werden anfänglich durch den Hauptvertrag zur Leistungserbringung festgelegt und können vom Auftraggeber danach schriftlich oder in Textform (z.B. E-Mail) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Hauptvertrag zur Leistungserbringung nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform vom Auftraggeber zu bestätigen.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf personenbezogene Daten, die Gegenstand des Auftrags sind, nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor und dessen Voraussetzungen werden gewahrt.

(2) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

(3) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Pseudonymisierung, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Die Einzelheiten zu den technischen und organisatorischen Maßnahmen sind in **Anhang 1** geregelt und orientieren sich an folgenden Datenschutz-Geboten:

a. **Pseudonymisierung** (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

   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 entsprechenden technischen und organisatorischen Maßnahmen unterliegen;

b. **Vertraulichkeit** (Art. 32 Abs. 1 lit. b DS-GVO)

   i. Zutrittskontrolle
   Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
   ii. Zugangskontrolle
   Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
   iii. Zugriffskontrolle
   Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
   iv. Trennungskontrolle
   Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

c. **Integrität** (Art. 32 Abs. 1 lit. b DS-GVO)

   i. Weitergabekontrolle
   Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
   ii. Eingabekontrolle
   Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

d. **Verfügbarkeit und Belastbarkeit** (Art. 32 Abs. 1 lit. b DS-GVO)

   i. Verfügbarkeitskontrolle
   ii. Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;
   iii. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

e. **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

   i. Datenschutz-Management;
   ii. Incident-Response-Management;
   iii. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
   iv. Auftragskontrolle

f. **Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers**, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(4) Soweit vereinbart unterstützt der Auftragnehmer den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten. Der Auftragnehmer führt diese Unterstützung bis zu einem Aufwand von vier Stunden unentgeltlich durch. Größere Aufwände bedürfen einer gesonderten Vereinbarung zwischen den beiden Vertragsparteien.

Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen. Der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten gemäß der geltenden Preisliste für Dienstleistungen.

(5) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(6) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden.

Eine Meldung von Datenschutzverletzungen muss mindestens enthalten:

- eine Beschreibung des Vorfalls, soweit möglich mit Angabe der Art der Verletzung des Schutzes personenbezogener Daten, Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
- eine Beschreibung der wahrscheinlichen Folgen des gemeldeten Vorfalls, eine Beschreibung der ergriffenen Maßnahmen zur Behebung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(7) Der Auftragnehmer nennt dem Auftraggeber den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen. Datenschutzbeauftragter des Auftragnehmers ist:

- Herr André Maslo, Telefon Durchwahl -207, andre.maslo@thinking-networks.com

(8) Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen.

(9) Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten (mit Ausnahme von routinemäßig gesicherten Kopien in Backups), wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe. Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Hauptvertrag zur Leistungserbringung bereits vereinbart. Auch insoweit erstattet der Auftraggeber dem Auftragnehmer die entstandenen Kosten gemäß der jeweils gültigen Preisliste Service.

(10) Nach Auftragsende sind sämtliche Daten zu löschen (mit Ausnahme von routinemäßig gesicherten Kopien in Backups) sowie vom Auftraggeber erhaltene Datenträger und sämtliche sonstige Materialien entweder herauszugeben oder zu vernichten. Entstehen dabei durch besondere Vorgaben zusätzliche Kosten, so erstattet diese der Auftraggeber gemäß der jeweils gültigen Preisliste Service.

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DS-GVO, gilt § 3 Abs. 4 entsprechend.

§ 5 Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Anträgen gemäß Art. 15-21 DS-GVO an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen und leitet den Antrag an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung dieser Anträge der betroffenen Personen im erforderlichen Umfang.

§ 6 Nachweismöglichkeiten

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach. Der Auftragnehmer verpflichtet sich, dem

Auftraggeber auf Aufforderung die dokumentierten Kontrollen und erforderlichen Auskünfte zur Verfügung zu stellen. Insbesondere ist die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO nachzuweisen.

(2) Der Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten kann erfolgen durch

- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)
- Selbstaudits
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, ISO 27001, ISO 27018, ISO 27701, VDS 10000)
- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO

(3) Kontrollrechte

a. Der Auftragnehmer verpflichtet sich, den Auftraggeber bei seinen Prüfungen gemäß Art. 28 Abs. 3 S. 2 lit. h DS-GVO zur Einhaltung der Vorschriften zum Datenschutz sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang zu unterstützen.
b. Die Prüfungen werden durch den Auftraggeber selbst oder einen von ihm beauftragten Dritten durchgeführt. Sollte der durch den Auftraggeber beauftragte Dritte in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht. Beauftragte Dritte müssen durch den Auftraggeber zur Verschwiegenheit verpflichtet werden. Dem Auftragnehmer steht das Recht zu, die Abgabe einer separaten Verschwiegenheitserklärung des beauftragten Dritten zu verlangen. Dies gilt insbesondere für die Abgabe von Erklärungen zur berufsrechtlichen oder gesetzlichen Verschwiegenheit.
c. Eine Prüfung kann insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch weitere Maßnahmen erfolgen. Zu den weiteren Maßnahmen zählen die Anforderung von Zertifizierungen, Berichte zu Datenschutzaudits und Inspektionen vor Ort. Inspektionen vor Ort nimmt der Auftraggeber mit angemessener Vorankündigung während der üblichen Geschäftszeiten vor. Die Prüfungen müssen ohne Störung des Betriebsablaufs sowie unter Wahrung der Sicherheits- und Vertraulichkeitsinteressen des Auftragnehmers durchgeführt werden und sind auf eine Prüfung pro Kalenderjahr beschränkt. Ausgenommen sind anlassbezogene Kontrollen. Der Auftraggeber erstattet dem Auftragnehmer die durch die Durchführung der Prüfung entstandenen Kosten, sofern diese den typischerweise zu erwartenden Umfang übersteigen.

§ 7 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Hauptvertrag zur Leistungserbringung vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. für Telekommunikationsleistungen, Post-/Transportdienstleistungen,

Wartung oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software in Anspruch nimmt, sofern ein Zugriff auf personenbezogene Daten ausgeschlossen werden kann.

(3) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung folgender Subunternehmer durchgeführt:

Buhl Data Service GmbH Am Siebertsweiher 3/5 57290 Neunkirchen	Bereitstellung, (Fern-)Wartung und Administration von IT-Systemen und -Infrastruktur

Vor der Hinzuziehung weiterer oder der Ersetzung aufgeführter Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung – innerhalb einer Frist von 4 Wochen – aus wichtigem Grund – gegenüber der vom Auftragnehmer bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben.

(4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.

§ 8 Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlichem« im Sinne der Datenschutz-Grundverordnung liegen.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Bei etwaigen Widersprüchen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen des Hauptvertrages zur Leistungserbringung vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.

(4) Es gilt deutsches Recht.

§ 9 Haftung und Schadensersatz

(1) Eine zwischen den Parteien im Hauptvertrag zur Leistungserbringung vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, außer soweit ausdrücklich etwas anderes vereinbart wurde.

(2) Soweit keine Haftungsregelung vereinbart wurde, haften Auftraggeber und Auftragnehmer gegenüber betroffenen Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

§ 10 Inkrafttreten

Diese Vereinbarung tritt mit Abschluss der elektronischen Registrierung zur Nutzung der Software QVANTUM als Software as a Service in Kraft. Vor Abschluss der elektronischen Registrierung ist keine Nutzung der Software QVANTUM als Software as a Service möglich.

Stand: 1. Juli 2023

Anhang 1 – Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

Technische und Organisatorische Maßnahmen

nach Art. 32 Abs. 1 DSGVO

English translation below.

Die Thinking Networks AG (Thinking Networks) möchte Personen davor schützen, dass sie durch den Umgang mit ihren personenbezogenen Daten in ihren Persönlichkeitsrechten verletzt werden. Dies betrifft sowohl die personenbezogenen Daten, die Thinking Networks zu eigenen Geschäftszwecken erhebt, verarbeitet und nutzt (z.B. Kunden- und Mitarbeiterdaten), als auch personenbezogene Daten, mit denen Mitarbeiter von Thinking Networks im Rahmen einer Auftragsdatenverarbeitung in Kontakt kommen.

Alle Mitarbeiter von Thinking Networks haben sich zur Wahrung der Vertraulichkeit und zur Beachtung des Datenschutzes verpflichtet, im Rahmen ihrer Beschäftigung bei Thinking Networks personenbezogene Daten nicht unbefugt zu erheben, zu verarbeiten oder zu nutzen. Diese Verpflichtung gilt für jeden Mitarbeiter ab Beginn seiner Tätigkeit für Thinking Networks und ist zeitlich unbegrenzt. Diese Verpflichtung bleibt über die Beendigung der Beschäftigung bei Thinking Networks hinaus bestehen.

Darüber hinaus hat die Thinking Networks weitere allgemeine Sicherheitsmaßnahmen ergriffen. Diese werden im nächsten Abschnitt beschrieben.

Im Rahmen der Auftragsdatenverarbeitung für Kunden können Mitarbeiter von Thinking Networks in Kontakt mit personenbezogenen Daten des Kunden kommen. Diesem Aspekt wird aufgrund der besonders sensiblen Daten besondere Aufmerksamkeit geschenkt. Einzelheiten zu Art, Umfang und Regelungen bei Auftragsdatenverarbeitung im Auftrag von Thinking Networks-Kunden ergeben sich aus den jeweiligen Auftragsdatenverarbeitungsverträgen.

Betrieblicher Datenschutzbeauftragter

Die Umsetzung des geltenden Datenschutzrechtes und die Einhaltung der Sicherheitsmaßnahmen werden durch den betrieblichen Beauftragten für den Datenschutz kontrolliert. Der betriebliche Beauftragte für den Datenschutz der Thinking Networks AG ist:

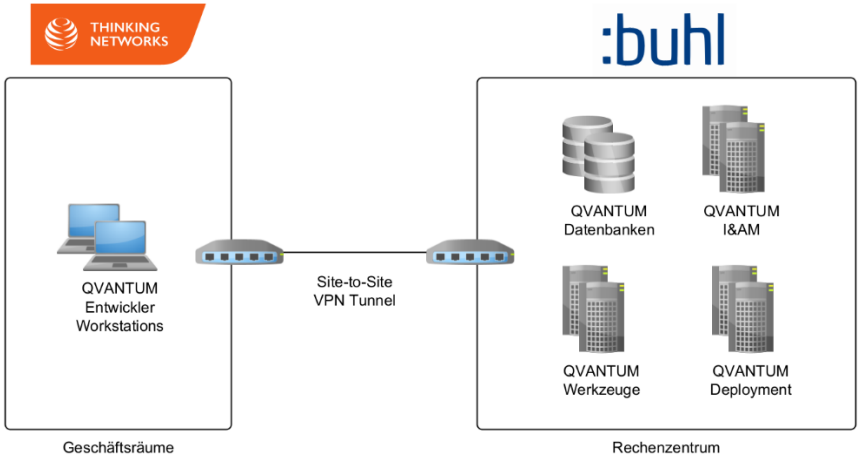
André Maslo
Thinking Networks AG
Markt 45 - 47
52062 Aachen
Tel. 0241 / 47072 - 0

E-Mail: andre.maslo@thinking-networks.com

Herr Maslo hat an einem Lehrgang zu den Themen Datenschutz und Datensicherheit teilgenommen und sich anschließend über eine Prüfung zum Datenschutzbeauftragten (TÜV) qualifiziert.

Inhaltsverzeichnis

Aufbau des Dokuments & IT-Topologie



Die Entwicklung von QVANTUM findet in den Geschäftsräumen der Thinking Networks AG (TN) Zentrale in Aachen statt. Die Buhl Data Service (BDS) ist die Muttergesellschaft der TN und stellt ihrer Tochter im eigenen Rechenzentrum die für Entwicklung und Betrieb von QVANTUM notwendige technische Basisinfrastruktur inkl. einer Reihe von Managed Services (z. B. Datenbank-Verwaltung, Recovery Strategien, Sicherheitsupdates) zur Verfügung. Darauf aufbauend verwalten die Mitarbeiter der Thinking Networks AG sowohl Entwicklungswerkzeuge als auch den Betrieb von QVANTUM. Der Betrieb von QVANTUM findet ausschließlich in einem nach VdS 10000 (https://vds.de/cyber/vds10000) zertifizierten Bereich des Rechenzentrums der Buhl Data Service statt.

Die folgenden Abschnitte beschreiben entsprechende technische und organisatorische Maßnahmen, aufgeschlüsselt nach den jeweiligen Standorten, gekennzeichnet mit „**TN**“ und „**BDS**“. Abschnitte 1-4

beschreiben im Wesentlichen die für QVANTUM angewandten Sicherheitsmaßnahmen im Rechenzentrum der Buhl Data Service in Deutschland. Die Abschnitte 5-7 enthalten ausführliche Hinweise zu besonders relevanten Sicherheitsaspekten, die nicht nur den Standort des Rechenzentrums, sondern auch den Standort der Entwicklung betreffen.

1. Pseudonymisierung und Verschlüsselung Personenbezogener Daten (BDS)

- HTTPS-Verschlüsselung in der Webkommunikation (Data-at-Transport)
- Verschlüsselung/Nutzung von VPN-Tunneln bei Übertragungen (Data-at-Transport)
- Pseudonymisierung wichtiger Daten (Data-at-Rest)

2. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste (BDS)

- I&AM pro Mandant gemäß den Standards OpenID Connect, OAuth2 und SAML 2.0
- Eigene Datenbanken pro Mandant
- Zugang zu Systemen nur mit individuellen Benutzernamen und Kennwörtern
- Berechtigte können nur auf für sie berechtigte Daten zugreifen
- Personenbezogene gespeicherte Daten können nur im Rahmen des Berechtigungskonzepts gelesen, kopiert, verändert oder entfernt werden
- Verwendung fortlaufend aktualisierter Virenschutzsoftware
- Schutz des E-Mail-Verkehrs vor Viren und Spam
- Firewallsysteme
- Sicherstellung einer hohen Widerstandsfähigkeit der DV-Systeme bei starkem Zugriff bzw. starker Belastung, etwa durch Angriffe von außen
- Verwendung ausgetesteter Software
- Trennung Produktiv- von Test- und Entwicklungsumgebung
- Sperren von externen Schnittstellen (USB, DVD-LW)
- Einsatz eines Intrusion-Detection-System
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Klimaanlagen in Serverräumen
- Load-Balancing
- Alert-Meldung bei hoher Belastung und Ausfällen mit SMS-Benachrichtigung von IT Personal
- Virtualisierung/Dynamische Zuteilung
- Hohe Passwortsicherheit, Regelmäßiger Wechsel
- Kein Zugang für Unbefugte zu den Datenverarbeitungsanlagen des Rechenzentrums
- Während der Geschäftszeiten Zutritt zu Geschäftsräumen durch Mitarbeiter kontrolliert
- Besucher der Rechenzentren werden begleitet
- Festlegung der berechtigten Personen in Listen für die sensiblen Bereiche der Rechenzentren
- Einbruchschutzmaßnahmen, Alarmanlage mit Aufschaltung auf Wachdienst
- Protokollierung der Besuche der Rechenzentren
- Definierter Kreis von Zugangsberechtigten
- Anzahl der Admins aufs Notwendigste begrenzt
- Sichere Löschung von Datenträgern
- Verbot der Nutzung privater Datenträger
- Empfang besetzt während Geschäftszeiten
- Videoüberwachung
- Regelungen zur Beschaffung von Hard-und Software
- Zentrales Rechtemanagement für Arbeitsplatz-PCs
- Regelung und Kontrolle von externer Wartung und Fernwartung

- Regelungen für Heimarbeitsplätze
- Brandmeldeanlage mit Aufschaltung auf Feuerwehrleitstelle

3. Verfügbarkeit Personenbezogener Daten und Zugang bei Zwischenfällen (BDS)

- Doppelt- oder Mehrfachvorhaltung aller Komponenten bei der Datenverarbeitung
- Datensicherung und Spiegelung von Hardwarekomponenten
- Datensicherungs- und Wiederherstellungskonzept
- Personenbezogene Daten sind ständig verfügbar und geschützt gegen zufällige Zerstörung oder Verlust durch regelmäßiges Backup
- Sicherheitskopien
- Besonders geschützte Rechenzentrumsabschnitte
- Unterbrechungsfreie Stromversorgung
- Redundante Stromzuführungen
- Überwachungs- und Meldesysteme
- Vertretungspläne für Personal

4. Überprüfung, Bewertung und Evaluierung der Wirksamkeit (BDS)

- Regelmäßige Prüfung, ob/in welchem Umfang Zugangsrechte noch erforderlich sind
- Regelmäßige Prüfung, ob/in welchem Umfang Zugriffsrechte noch erforderlich sind
- Incident-Response-Management
- Auftragskontrolle bei Auftragsverarbeitung
- Beauftragung von externen oder internen Prüfberichten
- Durchführung von notwendigen Anpassungsmaßnahmen

5. Detailliertere Hinweise zu unseren Sicherheitsmaßnahmen (TN, BDS)

5.1 Zutrittskontrolle (TN)

Der Zutritt zu den Geschäftsräumen von Thinking Networks erfolgt ausschließlich durch den zentralen Eingang. Die Tür zum zentralen Eingang wird durch ein elektronisches Sicherheitssystem mit Chip-Schlüsseln kontrolliert. Dabei wird festgehalten, welcher Chip-Schlüssel zu welchem Zeitpunkt eine Freigabe der Eingangstür bewirkt. Die Auswertung der Zutrittsprotokolle über entsprechende Listen ist möglich. Die Verwaltung der Chip-Schlüssel obliegt der Verwaltung des Bürogebäudes. Die Geschäftsräume sind i.d.R. montags bis freitags von 9:00 bis 18:00 Uhr besetzt.

5.2 Zugangskontrolle (TN)

Ziel der Zugangskontrolle ist es, zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden, mit denen die Verarbeitung und Nutzung personenbezogener Daten durchgeführt werden.

Der Internet-Zugang erfolgt über ein Security-Gateway mit einer integrierten Firewall. Das Security-Gateway macht interne Systeme über NAT aus dem Internet ausschließlich über das Secure Hypertext Transfer Protocol (HTTPS) erreichbar. Die integrierte Firewall erlaubt nur die Kommunikation der notwendigen Dienste, sowohl aus dem WAN in das LAN als auch aus dem LAN in das WAN.

Per Policy dürfen personenbezogene Daten ausschließlich auf Servern im internen Netzwerk gespeichert werden. Die Speicherung personenbezogener Daten auf Festplatten von Mitarbeiter-Notebooks ist Mitarbeitern explizit untersagt.

Die Sicherheit der Datenverarbeitungssysteme im Netzwerk beruht auf dem Sicherheitskonzept von Windows Active Directory Domänen. Der Zugang zu Maschinen und Diensten sowohl bei TN als auch im Buhl Rechenzentrum ist nur für eingetragene Benutzer über Ein-Faktor oder Multi-Faktor Authentifizierung möglich. Um Zugang zu im Netzwerk gespeicherten Daten zu erlangen, muss eine Anmeldung an einer der Domänen (TN oder Buhl) erfolgen. Jegliche Zugriffe von TN Mitarbeitern auf die Infrastruktur im Buhl Rechenzentrum erfolgt über einen speziell abgesicherten Site-to-Site VPN Tunnel.

TN Mitarbeiter haben die Möglichkeit, extern über eine Point-to-Site VPN-Verbindung mit ihren Entwickler Workstations auf das interne Netzwerk zuzugreifen. Hierbei handelt es sich um eine 256 Bit AES SSL-VPN Verbindung. Zum Aufbau einer Verbindung sind spezielle Authentifizierungsinformationen notwendig, oft in Verbindung mit einer Multi-Faktor Authentifizierung.

- Arbeitsplatz (**TN**)

  Thinking Networks hat seine Mitarbeiter angewiesen, dass beim Verlassen des Arbeitsplatzes der Bildschirm zu sperren ist sowie Dokumente mit personenbezogenen Daten in verschlossenen Schränken zu verwahren sind. Diese Anweisung wurde an alle Mitarbeiter von Thinking Networks (z.B. auch an die für die Hotline und die Fernwartung zuständigen Mitarbeiter) erteilt. Eine Sperrung des unbenutzten Rechners erfolgt automatisch nach fünf Minuten.

5.3 Zugriffskontrolle (TN, BDS)

Die Maßnahmen zur Zugriffskontrolle sind darauf gerichtet, dass nur auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Für firmeneigene Computer wurde ein DHCP-Pool eingerichtet, der bestimmte IP-Adressen nur an Computer vergibt, deren MAC-Adresse bekannt und hinterlegt ist. Ein direktes Aufschalten auf das Netzwerk mittels einer Netzwerkkabelverbindung ist somit nicht möglich. Das Anschließen nicht firmeneigener Rechner ist nichterlaubt.

- Netzwerk-Domänen (**TN, BDS**)

  Um Zugriff auf im Netzwerk gespeicherte Daten zu erlangen, muss eine Anmeldung an einer Domäne erfolgen. Innerhalb der Domäne wurden neben den Windows-Standardbenutzergruppen (Domänen-Admins, Domänen-Benutzer) spezielle Benutzergruppen eingerichtet, um beispielsweise nur dem Entwicklungsteam von Thinking Networks den Zugang zum Entwicklungssystem zu erlauben. Alleine die Administratoren bei TN und Buhl haben Root-Zugriff auf die Server. Freigaben auf Bereiche der Server werden von einem Administrator erteilt. Er kontrolliert, dass die Mitarbeiter entsprechend ihrer Zuordnung zu den unterschiedlichen Aufgabenbereichen nur auf die jeweils erforderlichen Ressourcen zugreifen können. Zum Arbeiten mit der aktuellen Entwicklungsumgebung sind

erhöhte Rechte notwendig. Diese wurden für Entwickler nur jeweils lokal für den eigenen Rechner-Arbeitsplatz vergeben.

- Rollenbasierte Benutzerautorisierung bei internen Softwaresystemen (**TN**)

  Über den Zugang zum Netzwerk hinaus ist auch der Zugang zu den internen Softwaresystemen durch Passwörter geschützt. Alle Softwaresysteme verfügen über eine rollenbasierte Benutzerautorisierung, mit der geregelt wird, dass der jeweilige Benutzer nur Zugang zu den Daten bekommt, die er zur Ausübung seiner Funktion benötigt. Die Zuordnung von Benutzern zu Rollen ist den Administratoren vorbehalten.

5.4 Trennungskontrolle (TN)

Ziel der Trennungs- oder Verwendungszweckkontrolle ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden. Die internen Datenverarbeitungsverfahren mit personenbezogenen Daten laufen auf getrennten Softwaresystemen mit separaten Datenbanken. Die Trennung ist damit physikalisch gegeben.

Werden in Ausnahmefällen Daten von mehreren Kunden im Auftrag verarbeitet, so ist auch hier die Trennung der Daten gewährleistet: Die Software der Thinking Networks erfordert für jede Kundeninstallation bzw. jeden „Mandanten" eine eigene Datenbank. Eine Verknüpfung/ Mischung von personenbezogenen Daten mehrerer Auftraggeber ist damit unmöglich.

5.5 Verfügbarkeit und Belastbarkeit (BDS, TN)

Die Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO) enthält die Aspekte:

- Verfügbarkeitskontrolle
- Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust
- Rasche Wiederherstellbarkeit

Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Die Verfügbarkeitskontrolle betrifft die internen Datenverarbeitungsverfahren von Thinking Networks sowie die Datenbanken der Kundenkommunikation.

- Virenschutz, Firewall (**TN**)

  Für den Schutz vor Malware (Viren, Trojaner, Würmern, Spyware, etc.) wird im gesamten Netzwerk die Software ESET NOD32 Antivirus bzw. Endpoint Antivirus sowie ein Security-Gateway (Firewall / WEB-Security / Mail-Security / Network-Security) der Firma Sophos eingesetzt. Der Datenverkehr aus dem WAN in das LAN und aus dem LAN in das WAN wird vom Security-Gateway auf Malware gescannt. Die im Netzwerk eingesetzte Antivirussoftware schützt die lokalen Rechner und Server und verhindert die Verbreitung von Viren und Malware innerhalb des Netzwerkes. Automatische Update-Prozesse sind integriert.

- Datensicherung (**TN, BDS**)

  Es erfolgt eine regelmäßige Datensicherung gemäß interner Sicherungs- und Wartungspläne. Der ordnungsgemäße Ablauf der Sicherung wird überprüft. Sicherungen von Datenbanken werden zunächst (lokal) auf der Festplatte angelegt und anschließend von dort auf Band gesichert. Im Rechenzentrum erfolgt zudem eine tägliche Sicherung aller virtuellen Maschinen.

6. Auftragskontrolle (TN, BDS)

Auftragsdatenverarbeitung von personenbezogenen Daten findet bei Thinking Networks ausschließlich im Rahmen von konkreten Auftragsdatenverarbeitungsverträgen mit Thinking Networks-Kunden statt und wird durch den Datenschutzbeauftragten (siehe Seite 1) regelmäßig überwacht.

7. Thinking Networks Hotline (TN)

Thinking Networks hat eine telefonische Hotline für QVANTUM eingerichtet. Sie unterstützt den Auftraggeber durch Hinweise zur Störungsbeseitigung, Störungsvermeidung und Fehlerumgehung. Die zuständigen Mitarbeiter der Hotline sind für den Umgang mit personenbezogenen Daten in besonderem Maße sensibilisiert.

Stand: 01. Juli 2023

Data Processing Agreement (DPA)
in accordance with Article 28 General Data Protection Regulation (GDPR)

(electronic form of contract)

This English translation is only for convenience. Legally binding is the German „Vereinbarung zur Auftragsverarbeitung“ (see above).

Between

user of the software QVANTUM as software as a service

- Controller -

and

provider of the software QVANTUM as software as a service
(Thinking Networks AG, Markt 45-47, D-52062 Aachen)

- Processor -

regarding data processing pursuant to Art. 28 para. 3 of the EU General Data Protection Regulation (GDPR).

Preamble

This Agreement specifies the data protection obligations of the contracting parties resulting from the data processing which is described in detail in the main contract (hereinafter, the “Agreement”). It applies to all activities related to the main contract for the provision of services which includes the processing of the personal data (“Data”) of the Controller by the employees of the Processor or those authorized by the Processor.

§ 1 Scope, duration and specification of data processing

The scope and duration as well as the more detailed provisions on the type and purpose of the data processing on behalf of Controller shall be specified in the main contract. The data processing includes, but is not limited to, the following data in particular:

(1) Type of data

a. personal data (e.g. name, address, telephone, e-mail)
b. contract data (e.g. contract relationships)
c. Controller history
d. planning and controlling data

(2) Type and purpose of processing

a. maintenance,
b. customization of new versions to a changed program setting,
c. warranty,
d. hotline,
e. remote access,
f. support for Controller during test scenarios
g. provision of IT infrastructure, as well as storage and backup of data within the scope of the Processor's cloud hosting services,
h. diagnosis and maintenance via remote access in cases where the possibility of access to personal data cannot be excluded,
i. additional support services by separate agreement and remuneration

(3) Categories of data subjects

The group of data subjects affected by the processing of their personal data within the scope of this Contract includes:

a. Controllers
b. Employees

Personal data of the Controller that the Processor processes for its own business purposes shall not be the subject of this Agreement.

The term of this Agreement corresponds to the term of the main contract unless the provisions of this Agreement provide for obligations beyond that term.

§ 2 Scope and responsibilities

(1) Processor shall process Data on behalf of the Controller. Such data processing shall include all activities detailed in the main contract and its statement of work. Within the scope of this Agreement, only Controller shall be responsible for compliance with the applicable statutory requirements on data protection, including, but not limited to, the lawfulness of disclosing Data to Processor and the lawfulness of data processing on behalf of the Controller. The Controller shall be the »controller« in accordance with Art. 4 no. 7 GDPR. Data processing shall take place exclusively in a member state of the European Union or in another state party to the Agreement on the European Economic Area. The same shall apply to data processing by subcontractors pursuant to § 7 of this Agreement.

(2) The instructions shall initially be determined by the main contract for the provision of services and may thereafter be amended, supplemented or replaced by the Controller in writing or in text form (e.g. e-mail) to the office designated by the Processor with individual instructions (individual instruction). Instructions that are not provided in the main contract for the provision of services shall be treated as a request for a change in services. Oral instructions are to be confirmed immediately in writing or in text form by the Controller.

§ 3 Obligations of the Processor

(1) The Processor may only process personal data that are subject to the order within the scope of the order and the instructions of the Controller unless there is an exceptional case within the meaning of Art. 28 para. 3 a) GDPR and its requirements are met.

(2) The Processor shall inform the Controller without undue delay if he considers that an instruction violates applicable law. The Processor may suspend the implementation of the instruction until it has been confirmed or amended by the Controller.

(3) The Processor shall organize the internal organization within its area of responsibility in such a way that it complies with the special requirements of data protection. He shall take technical and organizational measures for the adequate protection of the Controller's data that comply with the requirements of the General Data Protection Regulation (Art. 32 GDPR). The Processor shall take technical and organizational measures to ensure the pseudonymization, confidentiality, integrity, availability and resilience of the systems and services in connection with the Processing on a permanent basis. The Controller is aware of these technical and organizational measures and is responsible for ensuring that they provide an adequate level of protection for the risks of the processed data. The details of the technical and organizational measures are regulated in **Annex 1** and are based on the following data protection principles:

a. **pseudonymization** (Art. 32 para. 1 a) GDPR; Art. 25 para. 1 GDPR)

   The data processing in such a way 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;

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

   i. Admission control
   No unauthorized access to data processing systems, e.g.: magnetic or chip cards, keys, electric door openers, plant security or gatekeepers, alarm systems, video systems;
   ii. Entry control
   No unauthorized system use, e.g.: (secure) passwords, automatic locking mechanisms, two-factor authentication, encryption of data media;
   iii. Access control
   No unauthorized reading, copying, modification or removal within the system, e.g.: Authorization concepts and needs-based access rights, logging of accesses;
   iv. Separation control
   Separate processing of data collected for different purposes, e.g. multi-client capability, sandboxing;

c. **integrity** (Art. 32 para. 1 b) GDPR)

   i. Transfer control
   No unauthorized reading, copying, modification or removal during electronic transmission or transport, e.g.: encryption, virtual private networks (VPN), electronic signature;
   ii. Input control
   Determining whether and by whom personal data has been entered, modified or removed from data processing systems, e.g.: logging, document management;

d. **availability and resilience** (Art. 32 para. 1 b) GDPR)

   i. Availability control
   ii. Protection against accidental or deliberate destruction or loss, e.g.: backup strategy (online/offline; on-site/off-site), uninterruptible power supply (UPS), virus protection, firewall, reporting channels and emergency plans;

iii. Rapid recoverability (Art. 32 para. 1 c) GDPR);

e. **Procedures for regularly review, assessment and evaluation** (Art. 32 para. 1 d) GDPR; Art. 25 para. 1 GDPR)

v. Privacy management;
vi. Incident response management;
vii. Privacy-friendly default setting (Art. 25 para. 2 GDPR);
viii. Mission control

f. **No data processing regarding to Art. 28 GDPR without corresponding instruction of the Controller**, e.g.: clear contract design, formalized order management, strict selection of the service provider, obligation to convince in advance, follow-up checks.

The Processor reserves the right to change the security measures, however, it must be ensured that the contractually agreed level of protection is still maintained.

(4) To the agreed extent, the Processor shall support the Controller within the scope of its possibilities in fulfilling the requests and claims of data subjects pursuant to Chapter III of the GDPR and in complying with the obligations set forth in Art. 33 to 36 GDPR. The Processor shall provide this support free of charge up to an effort of four hours. Larger efforts require a separate agreement between the two contracting parties.

In the event of a claim being made against the Processor by a data subject with regard to any claims pursuant to Art. 82 GDPR, the Processor shall support the Controller in defending the claim to the extent possible. The Controller shall reimburse the Processor for the costs incurred as a result of this support in accordance with the applicable service price list.

(5) The Processor warrants that the employees involved in the processing of the Controller's data and other persons working for the Processor are prohibited from processing the data outside the scope of the instruction. Furthermore, the Processor warrants that the persons authorized to process the personal data have committed themselves to confidentiality or are subject to an appropriate statutory duty of confidentiality. The confidentiality obligation shall continue to exist even after termination of the order.

(6) The Processor shall inform the Controller without undue delay if he becomes aware of any violations of the protection of Controller’s data.

A data breach notification shall include, at a minimum:

- a description of the incident, including, to the possible extent, the nature of the data breach, the categories and approximate number of data subjects, and the approximate number of affected data
- the name and contact details of the data protection officer or other point of contact for further information
- a description of the probable consequences of the reported incident, a description of the measures taken to remedy it and, if applicable, measures to mitigate its possible adverse effects

(7) The Processor shall provide the Controller with the name of the contact person for data protection issues arising within the scope of the contract. The data protection officer of the Processor is:

- Mr. André Maslo, Telephone extension -207, andre.maslo@thinking-networks.com

(8) The Processor shall ensure that he complies with its obligations pursuant to Art.32 para. 1 d) GDPR to implement a procedure for the regular review of the effectiveness of the technical and organizational measures to ensure the security of processing.

(9) The Processor shall correct or delete the contractual data (except for copies stored routinely in backups) if the Controller instructs to do so and this is covered by the scope of instructions. In special cases to be determined by the Controller, storage or handover shall take place. Remuneration and protective measures for this shall be agreed separately, unless already agreed in the contract. In this respect, the Controller shall also reimburse the Processor for the costs incurred in accordance with the applicable service price list.

(10) Upon termination of the Agreement all data shall be deleted (except for copies stored routinely in backups) and all data media and other materials received from Controller shall either be handed over or destroyed. If additional costs are incurred due to deviating specifications, the Controller shall reimburse these costs in accordance with the applicable service price list.

§ 4 Obligations of the Controller

(1) The Controller shall inform the Processor immediately and in detail if he discovers errors or irregularities in the results of the data processing with regard to data protection provisions.

(2) In the event of a claim against the Processor by a data subject with regard to any claims pursuant to Art. 82 GDPR, Section 3 (4) of this Agreement shall apply accordingly.

§ 5 Requests of Data Subjects

If a data subject contacts the Processor with requests pursuant to Art. 15 to 21 GDPR, the Processor will advise the data subject to submit the request to the Controller and shall forward the request to the Controller. The Processor shall assist the Controller in responding to such requests of the data subjects to the necessary extent.

§ 6 Evidence

(1) The Processor shall provide the Controller with appropriate evidence of compliance with the obligations set forth in this Agreement. The Processor shall provide the Controller with the documented controls and required information upon request. In particular, the implementation of the technical and organizational measures in accordance with Art. 32 GDPR must be proven.

(2) Evidence of compliance with the obligations set forth in this Agreement may be provided by

- current attestations, reports or report extracts from independent bodies (e.g. auditors, auditing, data protection officers, IT security department, data protection auditors, quality auditors)
- self-audits
- suitable certification by IT security or data protection audit (e.g., in accordance with the German BSI-Grundschutz, ISO 27001, ISO 27018, ISO 27701, VDS 10000)
- compliance with approved rules of conduct in accordance with Art. 40 GDPR
- certification in accordance with an approved certification procedure pursuant to Art. 42 GDPR

(3) Rights of control

a) The Processor shall support the Controller in its audits pursuant to Art. 28 para. 3 sentence 2 h) of the GDPR for compliance with the data protection provisions and the contractual agreements to the appropriate and necessary extent.

b) The audit shall be carried out by the Controller itself or by a third party commissioned by him. If the third party commissioned by the Controller is in a competitive relationship with the Processor, the Processor shall have a right of objection against the third party. Commissioned third parties must be bound to secrecy by the Controller. The Processor shall be entitled to demand that the commissioned third party submit a separate declaration of confidentiality. This applies in particular to the submission of declarations of professional or legal confidentiality.

c) An audit may be carried out especially by obtaining information and inspecting the stored data and the data processing programs, as well as by other measures. Further measures include requesting certifications, data protection audit reports and on-site inspections. On-site inspections shall be carried out by the Controller with reasonable advance notice during regular business hours. Audits shall be conducted without disrupting operations and in a manner that protects the security and confidentiality interests of the Processor and shall be limited to one audit per calendar year. Excepted from this are audits carried out on an ad hoc basis. The Controller shall reimburse the Contractor for the costs incurred by the performance of the inspection, insofar as these exceed the scope typically to be expected.

§ 7 Subcontractors (other processors)

(1) The use of subcontractors as further data processors shall only be permissible if the Controller has given its prior consent to.

(2) A subcontractor relationship requiring consent is given if the Contractor commissions other contractors to perform all or part of the service agreed in the main contract for the provision of the service. The Processor shall enter into agreements with these third parties to the extent necessary to ensure appropriate data protection and information security measures. This shall not include secondary services which the Processor uses, for example, for telecommunications services, postal/transport services, maintenance or the disposal of data carriers and other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software, provided that access to personal data can be excluded.

(3) The contractually agreed services or the partial services described below shall be performed using the following subcontractors:

Buhl Data Service GmbH Am Siebertsweiher 3/5 57290 Neunkirchen	Provisioning, (remote) maintenance and administration of IT systems and infrastructure

The Processor shall inform the Controller before using additional subcontractors or replacing the listed subcontractors. The Controller may object to the change - within a period of 4 weeks - for good cause - to the office designated by the Processor. If no objection is made within the period, the consent to the change shall be deemed to be given.

(4) If the Processor assigns orders to subcontractors, it shall be the responsibility of the Processor to transfer its data protection obligations under this Agreement to the subcontractor.

§ 8 Information obligations, written form requirement, choice of law

(1) If the Controller's data are threatened by attachment or seizure, by insolvency or composition proceedings or by other events or measures of third parties, the Processor shall inform the Controller thereof without undue delay. The Processor shall immediately inform all persons responsible in this context that the sovereignty and ownership of the data lies exclusively with the Controller as the "controller" within the meaning of the General Data Protection Regulation.

(2) Amendments and additions to this Agreement and all its constituent parts - including any warranties of the Processor - shall require a written agreement, which may also be in an electronic format (text form), and the express indication that it is an amendment or addition to this Agreement. This shall also apply to the waiver of this formal requirement.

(3) In the event of any contradictions, the provisions of this Agreement shall take precedence over the provisions of the main contract. Should individual parts of this Agreement be invalid, this shall not affect the validity of the rest of the Agreement.

(4) German law shall apply.

§ 9 Liability and damages

(1) A liability provision agreed between the parties in the main contract shall also apply to data processing, unless expressly agreed otherwise.

(2) Unless a liability provision has been agreed, the Controller and the Processor shall be liable to data subjects in accordance with the provision set out in Art. 82 GDPR.

§ 10 Effective date

This Agreement becomes effective upon conclusion of the electronic registration for the use of the Software QVANTUM as Software as a Service. It is not possible to use the QVANTUM software as a service before the electronic registration has been completed.

Status 1st July 2023

Annex 1 – Technical and organizational measures according to Art. 32 GDPR

Technical and Organizational Measures

According to Art. 32 para. 1 GDPR

This English translation is only for your convenience. Legally binding are the German „Technische und Organisatorische Maßnahmen“ (see above).

Thinking Networks AG (Thinking Networks) wants to protect individuals from violation of their personal rights due to the processing of their personal data. This concerns both to personal data that Thinking Networks collects, processes and uses for its own business purposes (e.g. customer and employee data) and to personal data that is processed by Thinking Networks employees as part of a data processing agreement (DPA).

All employees of Thinking Networks have committed to maintain confidentiality and to comply with data protection laws, not to collect, process or use personal data without authorization within the scope of employment at Thinking Networks. This obligation applies to every employee from the beginning of his or her employment at Thinking Networks and is in effect for an unlimited period of time. This obligation shall survive the termination of employment at Thinking Networks.

In addition, Thinking Networks has implemented other general security measures. These are described in the next section.

In case of data processing for customers, employees of Thinking Networks may have some contact with personal data of the customer. Due to the particularly sensitive data, special attention is paid to this aspect. For details on the type, scope and regulations for data processing on behalf of customers, please refer to the individual data processing agreement (DPA).

Company Data Protection Officer

The implementation of the applicable data protection law and compliance with the security measures are controlled by the company data protection officer. The company data protection officer of Thinking Networks AG is:

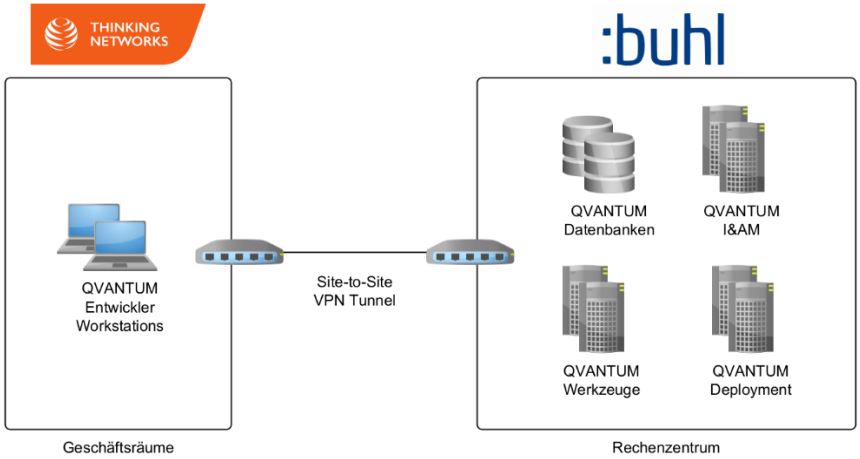
André Maslo
Thinking Networks AG
Markt 45 - 47
52062 Aachen (Germany)
Tel. + 49 241 / 47072 - 0

E-Mail: andre.maslo@thinking-networks.com

Mr. Maslo attended a training course on data protection and data security and then passed an examination to qualify as a data protection officer (TÜV).

Index

Document Structure & IT Topology



The development of QVANTUM takes place in the office of Thinking Networks AG (TN) in Aachen (Germany). Buhl Data Service (BDS) is the holding company and provides its subsidiary with the basic technical infrastructure required for the development and operation of QVANTUM, including a range of managed services (e.g. database administration, recovery strategies, security updates), in its own data center. Based on this, the employees of Thinking Networks AG manage development tools as well as the operation of QVANTUM. QVANTUM is operated exclusively in a VdS 10000 (https://vds.de/cyber/vds10000) certified area of the Buhl Data Service data center.

The following sections describe the relevant technical and organizational measures, classified by the relevant locations, marked with " **TN** " and " **BDS** ". Sections 1-4 mainly describe the security measures applied for QVANTUM at the Buhl Data Service data center in Germany. Sections 5-7

contain detailed information on particularly relevant security aspects that not only affect the location of the data center, but also the location of the development.

1. Pseudonymization & Encryption of Personal Data (BDS)

- HTTPS encryption in web communication (Data-at-Transport)
- Encryption/use of VPN-Tunnels for transmissions (Data-at-Transport)
- Pseudonymization of important data (Data-at-Rest)

2. Confidentiality, Integrity, Availability & Resilience of Systems and Services (BDS)

- I&AM per client according to OpenID Connect, OAuth2 and SAML 2.0 standards
- Own databases per client
- Access to systems only with individual user names and passwords
- Authorized persons can only access data authorized for them
- Personal data only be read, copied, changed or removed within scope of authorization concept
- Use of continuously updated virus protection software
- Protection of e-mail traffic against viruses and spam
- Firewall systems
- Ensuring a high level of resilience of data processing systems in the event of heavy load, e.g. by attacks from outside
- Use of tested software
- Separation of productive from test and development environments
- Blocking of external interfaces (USB, DVD-LW)
- Use of an intrusion detection system
- Obligation of employees to maintain data secrecy
- Air conditioning in server rooms
- Load balancing
- Alert message in case of high load and failures with SMS notification of IT staff
- Virtualization/dynamic allocation
- High password security, regular change
- No access for unauthorized persons to data processing facilities of the data center
- Access to business premises controlled by staff during business hours
- Visitors to the data centers are escorted
- Determination of authorized persons in lists for the sensitive areas of the data centers
- Anti-burglary measures, alarm system with connection to security service
- Logging of visits to the data centers
- Defined group of authorized persons
- Number of admins limited to the bare minimum
- Secure deletion of data media
- Prohibition of the use of private data media
- Reception staffed during business hours
- Video surveillance
- Regulations on the procurement of hardware and software
- Central rights management for workstation PCs
- Regulation and control of external and remote maintenance
- Regulations for home offices
- Fire alarm system with connection to fire department control center

3. Availability of Personal Data & Access in Case of Incidents (BDS)

- Duplication or multiple storage of all components during data processing
- Data backup and mirroring of hardware components
- Data backup and recovery concept
- Personal data is constantly available and protected against accidental destruction or loss through regular backup
- Backup copies
- Specially protected data center sections
- Uninterruptible power supply
- Redundant power supplies
- Monitoring and reporting systems
- Substitution plans for personnel

4. Review, Assessment & Evaluation of Effectiveness (BDS)

- Regular review of whether/to what extent entry control rights are still required
- Regular review of whether/to what extent admission control rights are still required
- Incident response management
- Order control for Data processing
- Commissioning of external or internal audit reports
- Implementation of necessary adaptation measures

5. More detailed Information about our Security Measures (TN, BDS)

5.1 Admission Control (TN)

Access to the offices of Thinking Networks is allowed only through the central entrance. The door of the central entrance is controlled by an electronic security system with chip keys. This system is used to record which chip key effects a release of the entrance door at which time. It is possible to evaluate the access logs via lists. The administration of the office building manages the chip keys. The business office is usually open from Monday to Friday from 9:00 to 18:00.

5.2 Entry Control (TN)

The purpose of entry control is to prevent data processing systems from being used by unauthorized persons to process and use personal data

Internet access is provided via a security gateway with an integrated firewall. The security gateway enables internal systems to be accessed via NAT from the Internet exclusively via the Secure Hypertext Transfer Protocol (HTTPS). The integrated firewall only allows communication of the necessary services, both from the WAN to the LAN and from the LAN to the WAN.

The data policy states that personal data may only be stored on servers located on the internal network. It is expressly forbidden for employees to store personal data on hard drives of employee notebooks.

The security of the data processing systems in the network is based on the security concept of Windows Active Directory domains. Access to machines and services at both TN and the Buhl data center is only possible for registered users via single-factor or multi-factor authentication. To gain access to data stored on the network, a login to one of the domains (TN or Buhl) is required. Any

access by TN employees to the infrastructure in the Buhl data center takes place via a specially secured site-to-site VPN tunnel.

TN employees have the opportunity to access the internal network externally via a point-to-site VPN connection with their developer workstations. This is a 256-bit AES SSL VPN connection. Special authentication information is required to establish a connection, often in connection with multi-factor authentication.

- Workplace (**TN**)

  Thinking Networks has instructed its employees to lock the screen when leaving the workplace and to keep documents containing personal data in closed lockers. This instruction has been provided to all employees of Thinking Networks (e.g. also to the employees responsible for the hotline and remote maintenance). Locking of the unused computer will automatically take place after five minutes.

5.3. Access Control (TN, BDS)

Access control measures are aimed to ensure that personal data can be accessed only with an existing authorization and that personal data cannot be read, copied, modified or removed during processing, use and after storage without authorization.

A DHCP pool has been set up for company-owned computers, which only assigns certain IP addresses to computers whose MAC address is known and stored. Therefore it is not possible to connect to the network via a network cable connection directly. It is not permitted to connect computers that are not company-owned.

- Network Domains (**TN, BDS**)

  In order to gain access to data stored on the network, a login to a domain is required. Within the domain, special user groups have been set up in addition to the standard Windows user groups (domain admins, domain users), for example, to allow only the Thinking Networks development team to access the development system. Only the administrators at TN and Buhl have root access to the servers. Approvals to areas of the servers are granted by an administrator. He or she controls that employees can only access the resources they need according to their assignment to the various task areas. To work with the current development environment increased rights are required. These rights have been assigned to developers only for their own computer workstations locally.
- Role-based user authorization for internal software systems (**TN**)

  In addition to access to the network, access to the internal software systems is also protected by passwords. All software systems have role-based user authorization, which ensures that the respective user only has access to the data he or she needs to perform his or her function. The assignment of users to roles is reserved for the administrators.

5.4 Separation Control (TN)

The purpose of separation or purpose of use control is to ensure that data collected for different purposes are processed separately. The internal data processing procedures with personal data operate on separate software systems with separate databases. Thus the separation is physically given.

In exceptional cases, data from several customers can be processed on behalf. Even in these cases, the separation of data is guaranteed: the software of Thinking Networks requires a separate database for each customer installation or "client". A linking/mixing of personal data of several clients is thus impossible.

5.5. Availability and Resilience (BDS, TN)

Availability and resilience (Art. 32(1)(b) GDPR) includes the following aspects:

- Availability control
- Protection against accidental or deliberate destruction or loss
- Rapid recovery

The purpose of availability control is to ensure that personal data is protected from accidental destruction or loss. Availability control concerns the internal data processing procedures of Thinking Networks as well as customer communication databases.

- Virus Protection, Firewall (**TN**)

  For protection against malware (viruses, Trojans, worms, spyware, etc.), the ESET NOD32 Antivirus or Endpoint Antivirus software and a security gateway (firewall / web security / mail security / network security) from Sophos are used in the entire network. The data traffic from the WAN to the LAN and from the LAN to the WAN is scanned for malware by the security gateway. The antivirus software used in the network protects the local computers and servers and prevents the spread of viruses and malware within the network. Automatic update processes are integrated.
- Data Backups (**TN, BDS**)
  A regular data backup is performed in accordance with internal backup and maintenance plans. The proper procedure of the backup is checked. Backups of databases are first created (locally) on the hard disk and then backed up from the disk to tape. In the data center, a daily backup of all virtual machines is also performed.

6. Order Control (TN, BDS)

At Thinking Networks, data processing of personal data takes place exclusively within the framework of specific data processing agreements with Thinking Networks customers (DPA) and is regularly monitored by the data protection officer (see page 7).

7. Support Hotline (TN)

Thinking Networks has established a telephone support hotline for QVANTUM. It provides support to the customer by giving advice on troubleshooting, fault avoidance and error workarounds. The employees responsible for the hotline are particularly aware of how to deal with personal data.

Status: 1st July 2023